kaspersky

Kaspersky Security Center Cloud Console

Inhalt

Online-Hilfe von Kaspersky Security Center Cloud Console

	**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-Programme: Regelmäßiges aktualisieren der Datenbanken und Programm-Module** Sorgen Sie für die ununterbrochene Zuverlässigkeit des Schutzsystems.
	**Lizenzierung von Kaspersky Security Center Cloud Console** Erfahren Sie mehr über die Verwendung von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console nach Ihren Bedürfnissen.		**Schwachstellen- und Patch-Management** Schwachstellen in Programmen von Drittanbietern finden und schließen.
	**Migration nach Kaspersky Security Center Cloud Console** Migrieren Sie Ihre vorhandenen Administrationsgruppen und deren zugehörigen Objekte und Einstellungen von dem lokalen Kaspersky Security Center auf Kaspersky Security Center Cloud Console.		**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.		**Kurzanleitung für Managed Service Provider (MSPs)** Erfahren Sie, wie Sie Kaspersky Security Center Cloud Console einsetzen können, wenn Sie Administrator eines MSPs sind.
	**Kaspersky-Programme: Zentralisierte Bereitstellung** Bereitstellung von Kaspersky-Programmen.		

Neuerungen

Update vom September 2023

Dieses Update von Kaspersky Security Center Cloud Console beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Kaspersky Security Center Cloud Console unterstützt jetzt Kaspersky Embedded Systems Security 3.3 für Linux.
- Kaspersky Security Center Cloud Console unterstützt jetzt Kaspersky Endpoint Security 12.2 für Windows.
- Optimierung der Benutzeroberfläche beim Arbeiten mit der Benutzerliste im Abschnitt **Geräte**.

Update vom Juni 2023

Dieses Update von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console und Ihre Netzwerkinfrastruktur zu konfigurieren.
- Kaspersky Security Center Cloud Console unterstützt jetzt Kaspersky Endpoint Security 11.3 für Mac.
- Kaspersky Security Center Cloud Console unterstützt jetzt Kaspersky Endpoint Security 11.4 für Linux.
- Darüber hinaus stehen Ihnen in Kaspersky Security Center Cloud Console 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 Security Center Cloud Console mit anderen Kaspersky-Programmen.
- 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 Security Center Cloud Console beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Kaspersky Security Center Cloud Console unterstützt jetzt Cluster und Server-Arrays als verwaltete Geräte. Wenn ein Kaspersky-Programm 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console folgende Funktionen zur Verfügung: Export von Richtlinien und Aufgaben in eine Datei, und anschließender Import von Richtlinien und Aufgaben in Kaspersky Security Center Windows oder Kaspersky Security Center Linux.

Update vom November 2022

Dieses Update von Kaspersky Security Center Cloud Console beinhaltet die folgenden neuen Funktionen und Verbesserungen:

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

Update vom Oktober 2022

Dieses Update von Kaspersky Security Center Cloud Console beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Wir haben den Inhalt der Vereinbarung zum Datenschutz für Kaspersky Security Center Cloud Console aktualisiert.
- Die Infrastruktur der Kaspersky Security Center Cloud Console benachrichtigt Sie jetzt über einen Arbeitsbereich, der keinen aktiven Lizenzschlüssel besitzt und der möglicherweise gelöscht wird, wenn Sie keinen neuen Lizenzschlüssel hinzufügen.
- Kaspersky Security Center Cloud Console unterstützt jetzt Kaspersky Endpoint Security 11.11.0 für Windows.
- Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 *Download von Updates in die Datenverwaltung der Verteilungspunkte* die Antiviren-Datenbanken für die Sicherheitsanwendungen von Kaspersky herunterzuladen.
- Der Administrationsagent ist jetzt in japanischer Lokalisierung verfügbar.
- In der Benutzeroberfläche der Kaspersky Security Center Cloud Console wurden die in Großbuchstaben ausgeschriebenen Abschnittsnamen an die gewöhnliche Groß- und Kleinschreibung angepasst.

Update vom August 2022

Neue Sprachunterstützung: Kaspersky Security Center Cloud Console steht jetzt vollständig in japanischer Sprache zur Verfügung.

Update vom Juli 2022

Dieses Update von Kaspersky Security Center Cloud Console beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Unterstützung der folgenden neuen Versionen von Kaspersky-Programmen:

- 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 Security Center Cloud Console aktualisiert.
- Zusätzliche Sprachunterstützung: Die Infrastruktur von Kaspersky Security Center Cloud Console ist jetzt in Japanisch verfügbar. Die Sprachunterstützung für Japanisch innerhalb der Arbeitsbereiche von Kaspersky Security Center Cloud Console folgt demnächst.

Update vom April 2022

Dieses Update von Kaspersky Security Center Cloud Console beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Kaspersky Security Center Cloud Console unterstützt jetzt Kaspersky Endpoint Security 11.9.0 für Windows.
- Kaspersky Security Center Cloud Console unterstützt jetzt die japanische Lokalisierung von Kaspersky Embedded Systems Security.

Update vom 9. März 2022

Dieses Update von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console verwalten.
- Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Kaspersky Security Center Cloud Console unterstützt jetzt Kaspersky Endpoint Detection and Response Optimum 2.0.
- Sie können jetzt mobile Android-Geräte mithilfe der Kaspersky Security Center Cloud Console verwalten.
- Der Kaspersky Marketplace ist als neuer Menüeintrag verfügbar: Sie können jetzt direkt in der Kaspersky Security Center Cloud Console nach neuen Kaspersky-Programmen suchen.
- Im Menü steht ein neuer Abschnitt namens Mitteilungen von Kaspersky zur Verfügung. Die Mitteilungen von Kaspersky informieren Sie über Wissenswertes zu den Kaspersky-Programmen, die auf Ihren verwalteten Geräten installiert sind. Die Informationen in diesem Abschnitt werden durch die Kaspersky Security Center Cloud Console regelmäßig aktualisiert.
- Sie können jetzt sekundäre Administrationsserver, die mit Linux betrieben werden, über die Kaspersky Security Center Cloud Console verwalten.

Update vom 7. September 2021

Dieses Update von Kaspersky Security Center Cloud Console beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Sie können jetzt Active Directory Federation Services (ADFS) verwenden, um sich unter Verwendung Ihres Active Directory-Benutzerkontos an Kaspersky Security Center Cloud Console anzumelden. Es muss kein neues Benutzerkonto mehr angelegt werden.
- Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console verbessert.

Update vom 27. Oktober 2020

Dieses Update von Kaspersky Security Center Cloud Console beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Kaspersky Security Center Cloud Console 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 Security Center Cloud Console beinhaltet die folgenden neuen Funktionen und Verbesserungen:

- Kaspersky Security Center Cloud Console unterstützt jetzt Kaspersky Security 11 für Windows Server (beginnend ab September 2020).

- Kaspersky Security Center Cloud Console 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 Security Center Cloud Console ist jetzt in italienischer Sprache verfügbar.

- Sie können jetzt den Endbenutzer-Lizenzvertrag (EULA) für jedes verwaltete Kaspersky-Programm über die Benutzeroberfläche von Kaspersky Security Center Cloud Console 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.

Kaspersky Security Center Cloud Console

Dieser Abschnitt informiert über die Konzeption, die wichtigsten Funktionen und die Programmkomponenten von Kaspersky Security Center Cloud Console.

Kaspersky Security Center Cloud Console ist ein Programm, das von Kaspersky gehostet und verwaltet wird. Sie müssen Kaspersky Security Center Cloud Console nicht auf Ihrem Computer oder Server installieren. Mit Kaspersky Security Center Cloud Console 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.

Über die Kaspersky Security Center Cloud Console

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

Mit Kaspersky Security Center Cloud Console können Sie Folgendes tun:

- Programme von Kaspersky auf Geräten Ihres Netzwerks installieren und die installierten Programme 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-Programmen 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 Security Center Cloud Console als mandantenfähige Anwendung verwenden.
- Kaspersky-Programme, die auf Client-Geräten installiert sind, remote verwalten.
- Die zentrale Bereitstellung von Lizenzschlüsseln für Kaspersky-Programme 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.

Sie verwalten Kaspersky Security Center Cloud Console mithilfe einer cloudbasierten Verwaltungskonsole, welche die Interaktion zwischen Ihrem Gerät und dem Administrationsserver über einen Browser sicherstellt. Beim Administrationsserver handelt es sich um ein Programm, das für die Verwaltung der auf Ihren Netzwerkgeräten installierten Kaspersky-Programme konzipiert ist. Wenn Sie mithilfe Ihres Browsers eine Verbindung zur Kaspersky Security Center Cloud Console herstellen, stellt der Browser eine sichere Verbindung mit dem Kaspersky Security Center Cloud Console Server 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 Security Center Cloud Console werden aktuell gehalten. Vom Administrationsserver und den erstellten Objekten (wie Richtlinien und Aufgaben) werden regelmäßig Sicherungskopien angelegt, um deren Schutz zu erhöhen.

Kaspersky Security Center Cloud Console ist eine mehrsprachige Anwendung. Sie können die Sprache der Benutzeroberfläche jederzeit und ohne erneutes Öffnen der Anwendung ändern.

Hardware- und Softwarevoraussetzungen für Kaspersky Security Center Cloud Console

Verwaltungskonsole

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

> Für die Arbeit mit Kaspersky Security Center Cloud Console kann nur ein einziges Browserfenster oder eine einzelne Registerkarte verwendet werden.

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

Browser:

- Mozilla Firefox Extended Support Release 91.8.0 oder höher (91.8.0 veröffentlicht am 5. April 2022)
- Google Chrome 100.0.4896.88 oder höher (offizieller Build)
- Microsoft Edge 100 oder höher
- Safari 15 auf macOS

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.

Softwarevoraussetzungen:

- Microsoft Windows Embedded POSReady 2009 mit dem aktuellsten Service Pack, 32-Bit
- Microsoft Windows Embedded POSReady 7 32-Bit/64-Bit
- Microsoft Windows Embedded 7 Standard mit Service Pack 1 32-Bit/64-Bit
- Microsoft Windows Embedded 8 Standard 32-Bit/64-Bit
- Microsoft Windows Embedded 8.1 Industry Pro 32-Bit/64-Bit
- Microsoft Windows Embedded 8.1 Industry Enterprise 32-Bit/64-Bit
- Microsoft Windows Embedded 8.1 Industry Update 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/ARM
- Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-Bit/ARM
- Microsoft Windows 10 Enterprise 2019 LTSC 32-Bit/64-Bit
- Microsoft Windows 10 IoT Enterprise Version 1703 32-Bit/64-Bit
- Microsoft Windows 10 IoT Enterprise Version 1709 32-Bit/64-Bit
- Microsoft Windows 10 IoT Enterprise Version 1803 32-Bit/64-Bit
- Microsoft Windows 10 IoT Enterprise Version 1809 32-Bit/64-Bit
- Microsoft Windows 10 20H2 IoT Enterprise 32-Bit/64-Bit
- Microsoft Windows 10 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 Home RS3 (Fall Creators Update, v1709) 32-Bit/64-Bit
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32-Bit/64-Bit
- Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, v1709) 32-Bit/64-Bit

- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32-Bit/64-Bit
- Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32-Bit/64-Bit
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32-Bit/64-Bit
- Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32-Bit/64-Bit
- Microsoft Windows 10 Pro for Workstations RS4 (April 2018 Update, 17134) 32-Bit / 64-Bit
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-Bit/64-Bit
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-Bit/64-Bit
- Microsoft Windows 10 Home RS5 (Oktober 2018) 32-Bit/64-Bit
- Microsoft Windows 10 Pro RS5 (Oktober 2018) 32-Bit/64-Bit
- Microsoft Windows 10 Pro für Workstations RS5 (Oktober 2018) 32-Bit/64-Bit
- Microsoft Windows 10 Enterprise RS5 (Oktober 2018) 32-Bit/64-Bit
- Microsoft Windows 10 Education RS5 (Oktober 2018) 32-Bit/64-Bit
- Microsoft Windows 10 Home 19H1 32-Bit/64-Bit
- Microsoft Windows 10 Pro 19H1 32-Bit/64-Bit
- Microsoft Windows 10 Pro für Workstations 19H1 32-Bit/64-Bit
- Microsoft Windows 10 Enterprise 19H1 32-Bit/64-Bit
- Microsoft Windows 10 Education 19H1 32-Bit/64-Bit
- Microsoft Windows 10 Home 19H2 32-Bit/64-Bit
- Microsoft Windows 10 Pro 19H2 32-Bit/64-Bit
- Microsoft Windows 10 Pro für Workstations 19H2 32-Bit/64-Bit
- Microsoft Windows 10 Enterprise 19H2 32-Bit/64-Bit
- Microsoft Windows 10 Education 19H2 32-Bit/64-Bit
- Microsoft Windows 10 Home 20H1 (Mai 2020 Update) 32-Bit/64-Bit
- Microsoft Windows 10 Pro 20H1 (Mai 2020 Update) 32-Bit/64-Bit
- Microsoft Windows 10 Enterprise 20H1 (Mai 2020 Update) 32-Bit/64-Bit
- Microsoft Windows 10 Education 20H1 (Mai 2020 Update) 32-Bit/64-Bit
- Microsoft Windows 10 Home 20H2 (Oktober 2020 Update) 32-Bit/64-Bit
- Microsoft Windows 10 Pro 20H2 (Oktober 2020 Update) 32-Bit/64-Bit

- Microsoft Windows 10 Enterprise 20H2 (Oktober 2020 Update) 32-Bit/64-Bit
- Microsoft Windows 10 Education 20H2 (Oktober 2020 Update) 32-Bit/64-Bit
- Microsoft Windows 10 Home 21H1 (Mai 2021 Update) 32-Bit/64-Bit
- Microsoft Windows 10 Pro 21H1 (Mai 2021 Update) 32-Bit/64-Bit
- Microsoft Windows 10 Enterprise 21H1 (Mai 2021 Update) 32-Bit/64-Bit
- Microsoft Windows 10 Education 21H1 (Mai 2021 Update) 32-Bit/64-Bit
- Microsoft Windows 10 Home 21H2 (Oktober 2021 Update) 32-Bit/64-Bit
- Microsoft Windows 10 Pro 21H2 (Oktober 2021 Update) 32-Bit/64-Bit
- Microsoft Windows 10 Enterprise 21H2 (Oktober 2021 Update) 32-Bit/64-Bit
- Microsoft Windows 10 Education 21H2 (Oktober 2021 Update) 32-Bit/64-Bit
- Microsoft Windows 11 Home 64-Bit
- Microsoft Windows 11 Pro 64-Bit
- Microsoft Windows 11 Enterprise 64-Bit
- Microsoft Windows 11 Education 64-Bit
- Microsoft Windows 11 22H2
- Microsoft Windows 8.1 Pro 32-Bit/64-Bit
- Microsoft Windows 8.1 Enterprise 32-Bit/64-Bit
- Microsoft Windows 8 Pro 32-Bit/64-Bit
- Microsoft Windows 8 Enterprise 32-Bit/64-Bit
- Microsoft Windows 7 Professional mit Service Pack 1 und höher, 32-Bit/64-Bit
- Microsoft Windows 7 Enterprise/Ultimate mit Service Pack 1 und höher, 32-Bit/64-Bit
- Microsoft Windows 7 Home Basic/Premium mit Service Pack 1 und höher, 32-Bit/64-Bit
- Microsoft Windows XP Professional Service Pack 3 und höher 32-Bit
- Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32-Bit
- Windows Small Business Server 2011 Essentials 64-Bit
- Windows Small Business Server 2011 Premium Add-on 64-Bit
- Windows Small Business Server 2011 Standard 64-Bit
- Windows MultiPoint Server 2011 Standard/Premium 64-Bit

- Windows MultiPoint Server 2012 Standard/Premium 64-Bit
- Windows Server 2008 Foundation mit Service Pack 2 32-Bit/64-Bit
- Windows Server 2008 Service Pack 2 (alle Versionen) 32-Bit/64-Bit
- Windows Server 2008 R2 Datacenter Service Pack 1 und höher, 64-Bit
- Windows Server 2008 R2 Enterprise Service Pack 1 und höher, 64-Bit
- Windows Server 2008 R2 Foundation mit Service Pack 1 und höher, 64-Bit
- Windows Server 2008 R2 mit Kernel-Mode Service Pack 1 oder höher 64-Bit
- Windows Server 2008 R2 Standard Service Pack 1 oder höher, 64-Bit
- Windows Server 2008 R2 Service Pack 1 (alle Editionen) 64-Bit
- Windows Server 2012 Server Core 64-Bit
- Windows Server 2012 Datacenter 64-Bit
- Windows Server 2012 Essentials 64-Bit
- Windows Server 2012 Foundation 64-Bit
- Windows Server 2012 Standard 64-Bit
- Windows Server 2012 R2 Server Core 64-Bit
- Windows Server 2012 R2 Datacenter 64-Bit
- Windows Server 2012 R2 Essentials 64-Bit
- Windows Server 2012 R2 Foundation 64-Bit
- Windows Server 2012 R2 Standard 64-Bit
- Windows Server 2016 Datacenter (LTSB) 64-Bit
- Windows Server 2016 Standard (LTSB) 64-Bit
- Windows Server 2016 Server Core (Installationsoption) (LTSB) 64-Bit
- Windows Server 2019 Standard 64-Bit
- Windows Server 2019 Datacenter 64-Bit
- Windows Server 2019 Core 64-Bit
- Windows Server 2022 Standard 64-Bit
- Windows Server 2022 Datacenter 64-Bit
- Windows Server 2022 Core 64-Bit

- Windows Storage Server 2012 64-Bit
- Windows Storage Server 2012 R2 64-Bit
- Windows Storage Server 2016 64-Bit
- Windows Storage Server 2019 64-Bit
- Debian GNU/Linux 11.x (Bullseye) 32-Bit/64-Bit
- Debian GNU/Linux 10.x (Buster) 32-Bit/64-Bit
- Debian GNU/Linux 9.x (Stretch) 32-Bit/64-Bit
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-Bit
- Ubuntu Server 20.04 LTS (Focal Fossa) 32-Bit/64-Bit
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64-Bit
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32-Bit/64-Bit
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-Bit/64-Bit
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-Bit/64-Bit
- CentOS 7.x 64-Bit
- CentOS 7.x ARM 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
- Red Hat Enterprise Linux Server 6.x 32-Bit/64-Bit
- SUSE Linux Enterprise Server 12 (alle Service Packs) 64-Bit
- SUSE Linux Enterprise Server 15 (alle Service Packs) 64-Bit
- SUSE Linux Enterprise Desktop 15 (alle Service Packs) 64-Bit
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64-Bit
- openSUSE 15 64-Bit
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64-Bit
- Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.7) 64-Bit
- Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.6) 64-Bit

- Astra Linux Common Edition (operatives Update 2.12) 64-Bit
- Astra Linux Special Edition RUSB.10152-02 (operatives Update 4.7) ARM 64-Bit
- Mageia 4 32-Bit
- Oracle Linux 7 64-Bit
- Oracle Linux 8 64-Bit
- Oracle Linux 9 64-Bit
- Linux Mint 19.x 32-Bit
- Linux Mint 20.x 64-Bit
- AlterOS 7.5 und höher, 64-Bit
- GosLinux IC6 64-Bit
- RED OS 7.3 64-Bit
- RED OS 7.3 Server 64-Bit
- RED OS 7.3 Certified Edition 64-Bit
- ROSA COBALT 7.9 64-Bit
- ROSA CHROME 12 64-Bit
- Lotos (Linux Core-Version 4.19.50, DE: MATE) 64-Bit
- macOS Sierra (10.12)
- macOS High Sierra (10.13)
- macOS Mojave (10.14)
- macOS Catalina (10.15)
- macOS Big Sur (11.x)
- macOS Monterey (12.x)

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

Die folgenden virtuellen Plattformen werden unterstützt:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro

- Microsoft Hyper-V Server 2012 64-Bit
- Microsoft Hyper-V Server 2012 R2 64-Bit
- Microsoft Hyper-V Server 2016 64-Bit
- Microsoft Hyper-V Server 2019 64-Bit
- Microsoft Hyper-V Server 2022 64-Bit
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Kernel-basierte virtuelle Maschine. Unterstützt die folgenden Betriebssysteme:
  - Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.7) 64-Bit
  - Debian GNU/Linux 11.x (Bullseye) 32-Bit/64-Bit
  - Ubuntu Server 20.04 LTS (Focal Fossa) 64-Bit
  - RED OS 7.3 64-Bit
  - RED OS 7.3 Server 64-Bit
  - RED OS 7.3 Certified Edition 64-Bit

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

Nicht unterstützte Betriebssysteme und Plattformen

Administrationsagent

Die folgenden Betriebssysteme werden nicht unterstützt:

- Microsoft Windows Embedded 8 Industry Pro 32-Bit/64-Bit
- Microsoft Windows Embedded 8 Industry Enterprise 32-Bit/64-Bit
- Microsoft Windows 10 Home (Threshold 1, 1507) 32-Bit/64-Bit
- Microsoft Windows 10 Pro (Threshold 1, 1507) 32-Bit/64-Bit
- Microsoft Windows 10 Enterprise (Threshold 1, 1507) 32-Bit/64-Bit
- Microsoft Windows 10 Education (Threshold 1, 1507) 32-Bit/64-Bit
- Microsoft Windows 10 Mobile (Threshold 1, 1507) 32-Bit

- Microsoft Windows 10 Mobile Enterprise (Threshold 1, 1507) 32-Bit
- Microsoft Windows 10 Home Threshold 2 (November 2015 Update, 1511) 32-Bit/64-Bit
- Microsoft Windows 10 Pro Threshold 2 (November 2015 Update, 1511) 32-Bit/64-Bit
- Microsoft Windows 10 Enterprise Threshold 2 (November 2015 Update, 1511) 32-Bit/64-Bit
- Microsoft Windows 10 Education Threshold 2 (November 2015 Update, 1511) 32-Bit/64-Bit
- Microsoft Windows 10 Mobile Threshold 2 (Update vom November 2015, 1511) 32-Bit
- Microsoft Windows 10 Mobile Enterprise Threshold 2 (November 2015 Update, 1511) 32-Bit
- Microsoft Windows 10 Home RS1 (Anniversary Update, 1607) 32-Bit/64-Bit
- Microsoft Windows 10 Pro RS1 (Anniversary Update, 1607) 32-Bit/64-Bit
- Microsoft Windows 10 Enterprise RS1 (Anniversary Update, 1607) 32-Bit/64-Bit
- Microsoft Windows 10 Education RS1 (Anniversary Update, 1607) 32-Bit/64-Bit
- Microsoft Windows 10 Mobile RS1 (Anniversary Update, 1607) 32-Bit
- Microsoft Windows 10 Mobile Enterprise RS1 (Anniversary Update, 1607) 32-Bit
- Microsoft Windows 10 Home RS2 (Creators Update, 1703) 32-Bit/64-Bit
- Microsoft Windows 10 Pro RS2 (Creators Update, 1703) 32-Bit/64-Bit
- Microsoft Windows 10 Enterprise RS2 (Creators Update, 1703) 32-Bit/64-Bit
- Microsoft Windows 10 Education RS2 (Creators Update, 1703) 32-Bit/64-Bit
- Microsoft Windows 10 Mobile RS2 (Creators Update, 1703) 32-Bit
- Microsoft Windows 10 Mobile Enterprise RS2 (Creators Update, 1703) 32-Bit
- Microsoft Windows 10 Mobile RS3 32-Bit
- Microsoft Windows 10 Mobile Enterprise RS3 32-Bit
- Microsoft Windows 10 Mobile RS4 32-Bit
- Microsoft Windows 10 Mobile Enterprise RS4 32-Bit
- Microsoft Windows 10 Mobile RS5 32-Bit
- Microsoft Windows 10 Mobile Enterprise RS5 32-Bit
- Microsoft Windows 8 (Core) 32-Bit/64-Bit
- Microsoft Windows 7 Professional 32-Bit/64-Bit
- Microsoft Windows 7 Enterprise/Ultimate 32-Bit/64-Bit

- Microsoft Windows 7 Home Basic/Premium 32-Bit/64-Bit
- Microsoft Windows Vista Business mit Service Pack 1 32-Bit/64-Bit
- Microsoft Windows Vista Enterprise mit Service Pack 1 32-Bit/64-Bit
- Microsoft Windows Vista Ultimate mit Service Pack 1 32-Bit/64-Bit
- Microsoft Windows Vista Business mit Service Pack 2 und höher, 32-Bit/64-Bit
- Microsoft Windows Vista Enterprise mit Service Pack 2 und höher, 32-Bit/64-Bit
- Microsoft Windows Vista Ultimate mit Service Pack 2 und höher, 32-Bit/64-Bit
- Microsoft Windows XP Professional mit Service Pack 2 32-Bit/64-Bit
- Microsoft Windows XP Home mit Service Pack 3 und höher, 32-Bit
- Windows Essential Business Server 2008 Standard 64-Bit
- Windows Essential Business Server 2008 Premium 64-Bit
- Windows Small Business Server 2003 Standard mit Service Pack 1 32-Bit
- Windows Small Business Server 2003 Premium mit Service Pack 1 32-Bit
- Windows Small Business Server 2008 Standard 64-Bit
- Windows Small Business Server 2008 Premium 64-Bit
- Windows Home Server 2011 64-Bit
- Windows MultiPoint Server 2010 Standard 64-Bit
- Windows MultiPoint Server 2010 Premium 64-Bit
- Microsoft Windows 2000 Server 32-Bit
- Windows Server 2003 Enterprise mit Service Pack 2 32-Bit/64-Bit
- Windows Server 2003 Standard mit Service Pack 2 32-Bit/64-Bit
- Windows Server 2003 R2 Enterprise mit Service Pack 2 32-Bit/64-Bit
- Windows Server 2003 R2 Standard mit Service Pack 2 32-Bit/64-Bit
- Windows Server 2008 Datacenter Service Pack 1 32-Bit/64-Bit
- Windows Server 2008 Enterprise Service Pack 1 32-Bit/64-Bit
- Windows Server 2008 Service Pack 1 Server Core 32-Bit/64-Bit
- Windows Server 2008 Standard Service Pack 1 32-Bit/64-Bit
- Windows Server 2008 Standard 32-Bit/64-Bit

- Windows Server 2008 Enterprise 32-Bit/64-Bit
- Windows Server 2008 Datacenter 32-Bit/64-Bit
- Windows Server 2008 R2 Server Core 64-Bit
- Windows Server 2008 R2 Datacenter 64-Bit
- Windows Server 2008 R2 Enterprise 64-Bit
- Windows Server 2008 R2 Foundation 64-Bit
- Windows Server 2008 R2 Standard 64-Bit
- Windows Server 2016 Nano (Installationsoption) (CBB)
- Windows Storage Server 2008 32-Bit/64-Bit
- Windows Storage Server 2008 Service Pack 2 64-Bit
- Windows Storage Server 2008 R2 64-Bit
- Debian GNU/Linux 7.x (bis 7.8) 32-Bit/64-Bit
- Debian GNU/Linux 8.x (Jessie) 32-Bit/64-Bit
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32-Bit/64-Bit
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32-Bit/64-Bit
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32-Bit/64-Bit
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-Bit/64-Bit
- CentOS 6.x (bis 6.6) 64-Bit
- CentOS 8.x 64-Bit
- SUSE Linux Enterprise Desktop 12 (alle Service Packs) 64-Bit
- Astra Linux Special Edition RUSB.10152-02 (operatives Update 4.7) ARM 64-Bit
- ALT Server 10 64-Bit
- ALT Server 9.2 64-Bit
- ALT Workstation 10 32-Bit/64-Bit
- ALT Workstation 9.2 32-Bit/64-Bit
- ALT 8 SP Server (LKNV.11100-01) 64-Bit
- ALT 8 SP Server (LKNV.11100-02) 64-Bit
- ALT 8 SP Server (LKNV.11100-03) 64-Bit

- ALT 8 SP Workstation (LKNV.11100-01) 32-Bit/64-Bit
- ALT 8 SP Workstation (LKNV.11100-02) 32-Bit/64-Bit
- ALT 8 SP Workstation (LKNV.11100-03) 32-Bit/64-Bit
- ROSA Enterprise Linux Server 7.3 64-Bit
- ROSA Enterprise Linux Desktop 7.3 64-Bit
- ROSA COBALT Workstation 7.3 64-Bit
- ROSA COBALT Server 7.3 64-Bit
- OS X 10.10 (Yosemite)
- OS X 10.11 (El Capitan)

Die folgenden Virtualisierungsplattformen werden nicht unterstützt:

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64-Bit
- Microsoft Hyper-V Server 2008 R2 64-Bit
- Microsoft Hyper-V Server 2008 R2 mit Service Pack 1 und höher, 64-Bit
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2

- Citrix XenServer 6.5
- Citrix XenServer 7

Programme und Lösungen von Kaspersky, die über die Kaspersky Security Center Cloud Console verwaltet werden können

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

Die folgenden Programme und Lösungen von Kaspersky können Sie über die Kaspersky Security Center Cloud Console bereitstellen und verwalten:

- Kaspersky Security für Windows Server 11.0.1
- Kaspersky Endpoint Security 12.2 für Windows
- Kaspersky Endpoint Security 11.4.0 für Linux
- Kaspersky Endpoint Security 11.3 für Mac
- Kaspersky Embedded Systems Security 3.2 für Windows
- Kaspersky Embedded Systems Security 3.3 für Linux
- Kaspersky Endpoint Agent 3.14
- Kaspersky Endpoint Security für Android
- Kaspersky Security für iOS

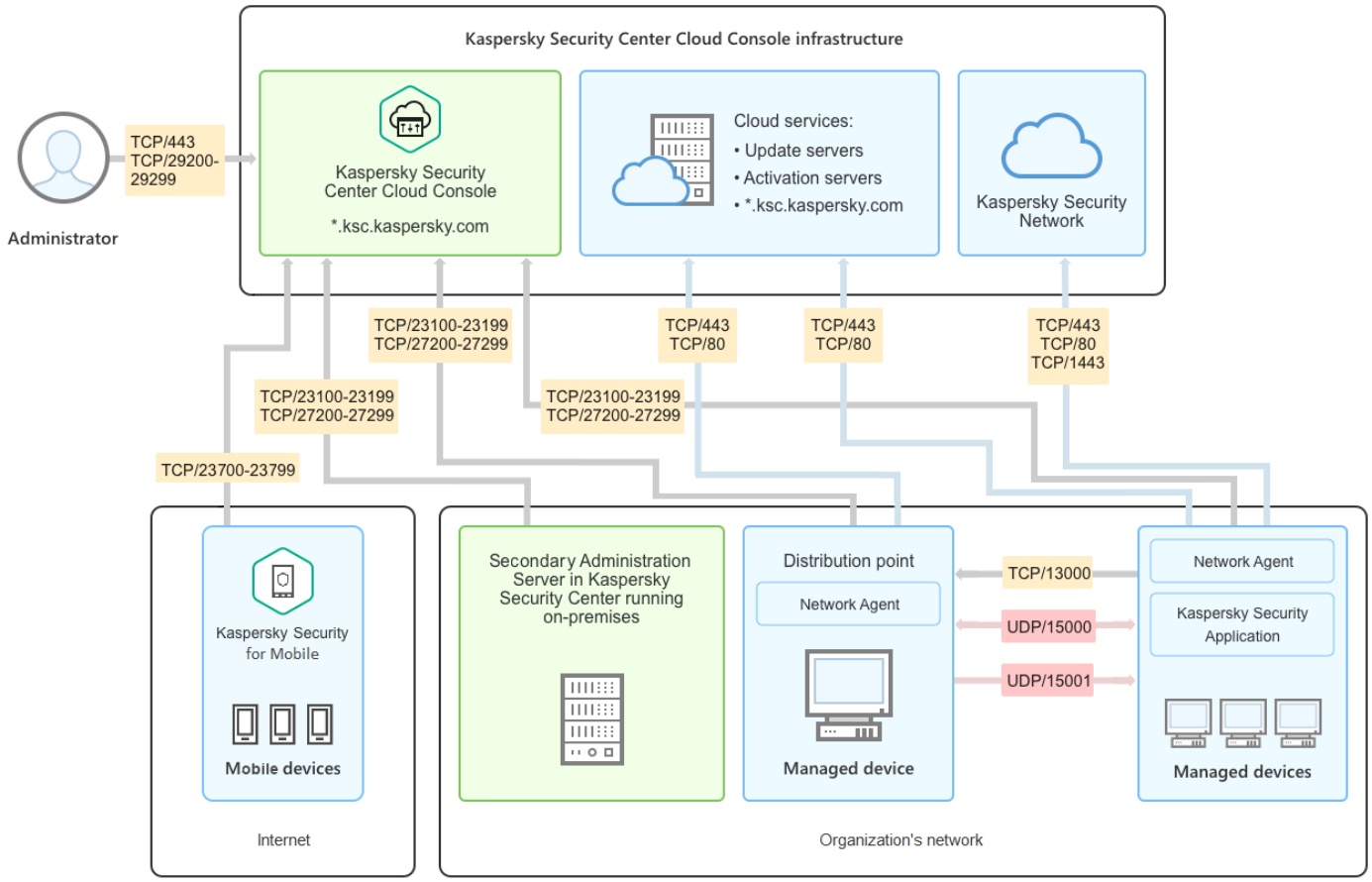
Die folgenden Lösungen können Sie integrieren, um Sicherheitsvorfälle anzuzeigen und zu bearbeiten:

- Kaspersky Managed Detection and Response
- Kaspersky Endpoint Detection and Response Optimum 2.3
- Kaspersky Endpoint Detection and Response Expert

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 Security Center Cloud Console bereit. Kaspersky Security Center Cloud Console kann diese Daten jedoch nicht verarbeiten wie im Abschnitt Durch verwaltete Anwendungen verarbeitete Daten der Dokumentation beschrieben. Damit Kaspersky Security Center Cloud Console diese Daten verarbeiten kann, müssen Sie für die neue Programmversion eine neue Richtlinie erstellen.

Architektur

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



Kaspersky Security Center Cloud Console-Architektur

Das durch die cloudbasierte Konsole verwaltete Kaspersky Security Center Cloud Console besitzt zwei Hauptkomponenten: Die Infrastruktur von Kaspersky Security Center Cloud Console und die Infrastruktur des Kunden.

Die Infrastruktur von Kaspersky Security Center Cloud Console umfasst:

- **Cloudbasierte Verwaltungskonsole**. Bietet eine Weboberfläche zum Erstellen und Verwalten des Schutzsystems in dem von Kaspersky Security Center Cloud Console 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 Programme von Kaspersky 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 ihnen manuell Verteilungspunkte zu.

- **Verwaltete Geräte**. Computer im Netzwerk des Kunden, die durch Kaspersky Security Center Cloud Console 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 Security Center Cloud Console verwendete Ports

Um Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console mit Programmen von Drittanbietern 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-	HTTPS	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver

Service auf dem Gerät ausgeführt wird)			

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 einem lokal ausgeführten Kaspersky Security Center verwendet werden. Nutzen Sie diese Ports für die Interaktion zwischen Ihrem sekundären Administrationsserver (oder Ihren sekundären Administrationsservern) und den Client-Geräten.

Benutzeroberfläche von Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console wird über eine Weboberfläche verwaltet.

Das Hauptfenster des Programms enthält die folgenden Elemente:

- Hauptmenü im linken Teil des Fensters
- Arbeitsbereich im rechten Teil des Fensters

Hauptmenü

Das Hauptmenü enthält die folgenden Abschnitte:

- **Einführung und Tutorials**. Enthält Videos zur Konfiguration und Verwendung von Kaspersky Security Center Cloud Console und den Sicherheitsanwendungen.
- **Administrationsserver**. Zeigt den Namen des Administrationsservers an, mit dem Sie aktuell verbunden sind. Klicken Sie auf das Einstellungssymbol (), um die Eigenschaften des Administrationsservers zu öffnen.
- **Überwachung und Berichterstattung**. Bietet Ihnen einen Überblick über die Infrastruktur, den Schutzstatus und die Statistiken.
- **Geräte**. Enthält Werkzeuge für die Verwaltung von Client-Geräten, sowie von Aufgaben und Richtlinien für Kaspersky-Programme.
- **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 Softwareverteilung**. Ermöglicht Ihnen Netzwerkabfragen durchzuführen, um Client-Geräte zu suchen, sowie die manuelle oder automatische Verteilung der 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 Security Center Cloud Console mit anderen Kaspersky-Programmen. Enthält auch Ihre persönlichen Einstellungen für das Design der Benutzeroberfläche, z. B. Sprache der Benutzeroberfläche oder das Farbschema.

- **Menü von Ihrem Benutzerkonto**. Enthält einen Link zur Online-Hilfe und Informationen über den Technischen Support von Kaspersky. Darüber hinaus können Sie sich von der Kaspersky Security Center Cloud Console abmelden.

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.

Lokalisierung von Kaspersky Security Center Cloud Console

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

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

Vergleich von Kaspersky Security Center und Kaspersky Security Center Cloud Console

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 Security Center Cloud Console. 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 Security Center Cloud Console vergleichen.

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

Funktion oder Eigenschaft	Kaspersky Security Center 14 wird on-premises ausgeführt	Kaspersky Security Center Cloud Console
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 Security Center Cloud Console 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 Security Center Cloud Console	✓	✓
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)
Schutz der Public-Cloud-Infrastruktur	✓	✓
Gerätezentrierte Sicherheitsverwaltung	✓	✓

Programmrichtlinien	✓	✓
Aufgaben für Kaspersky-Programme	✓	✓
Kaspersky Security Network	✓	✓
KSN-Proxyserver	✓	✓ (nur auf Verteilungspunkten)
Kaspersky Private Security Network	✓	–
Zentralisierte Bereitstellung von Lizenzschlüsseln für Kaspersky-Programme	✓	✓
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	✓	✓
Installieren von Software-Updates von Drittanbietern und Beheben von Schwachstellen in Programmen von Drittanbietern	✓	✓ (Um Sicherheitslücken in den Programmen von Drittanbietern 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 (abhängig von der Anzahl an verwalteten Geräten)
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	✓ (nur in der MMC-basierten Verwaltungskonsole)	–
Remote-Installation von Betriebssystemen	✓	–
SNMP-Unterstützung	✓	–

Grundbegriffe

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

Administrationsagent

Interaktion zwischen dem Administrationsserver und den Geräten wird mithilfe der Komponente *Administrationsagent* von Kaspersky Security Center Cloud Console durchgeführt. Der Administrationsagent muss auf allen Geräten installiert werden, auf welchen Kaspersky-Programme mittels Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console verwaltet werden können.

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

- Verwenden derselben Programmeinstellungen (die Sie in Gruppenrichtlinien festlegen können).
- Verwenden eines allgemeinen Betriebsmodus für alle Programme, indem Gruppenaufgaben mit festgelegten Einstellungen erstellt werden. Beispiele für Gruppenaufgaben umfassen unter anderem das Erstellen und Installieren eines Standard-Installationspakets, Aktualisieren von Programm-Datenbanken und Modulen, 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console stellen. Die restlichen verwalteten Geräte können unter Verwaltung des lokal ausgeführten Administrationsservers verbleiben. Dies erlaubt es Ihnen, die Verwaltungsfunktionen von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console, 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 Security Center Cloud Console unterstützt.

- Für virtuelle Administrationsserver können keine sekundären Administrationsserver angelegt werden (einschließlich virtueller Server).
- Virtuelle Administrationsserver können nicht von Kaspersky Security Center nach Kaspersky Security Center Cloud Console migriert werden.
- Virtuelle Administrationsserver können nicht durch dezidierte Server verwaltet werden. Der für die Verwaltung des primären Administrationsservers zuständige Administrator verwaltet standardmäßig auch die virtuellen Administrationsserver.
- 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. 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.
- Rolle des Gateways für die Verbindung mit dem Administrationsserver für Geräte in einer Administrationsgruppe übernehmen.

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

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

- Abfragen des Netzwerks, um neue Geräte und aktualisierte Informationen über die bereits bekannten Geräte zu finden.
- Ausführen der Remote-Installation von Programmen sowohl von Drittanbietern als auch von Kaspersky mit Microsoft Windows-Mitteln, 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.

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

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

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

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

Für die Ausführung des Verteilungspunkts sind mindestens 4 GB freier Speicherplatz auf dem Datenträger erforderlich. Wenn der freie Speicherplatz auf dem Datenträger des Verteilungspunkts weniger als 2 GB beträgt, erstellt Kaspersky Security Center Cloud Console einen Vorfall der Ereigniskategorie *Warnung*. Der Vorfall wird in den Eigenschaften des Geräts im Abschnitt **Vorfälle** 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 Security Center Cloud Console wird eine spezielle Komponente – das *Web-Plug-in zur Verwaltung* – verwendet. Im Weiteren wird das Web-Plug-in zur Verwaltung als *Verwaltungs-Plug-in* bezeichnet. Das Verwaltungs-Plug-in ist eine Schnittstelle zwischen Kaspersky Security Center Cloud Console und einem spezifischen Programm von Kaspersky. 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-Programmen und Geräten
- Übertragung von Ereignissen, die von der Anwendung erzeugt wurden
- Kaspersky Security Center Cloud Console 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 Kaspersky-Programmeinstellungen, die auf eine Administrationsgruppe und deren Untergruppen angewendet werden. Sie können mehrere Kaspersky-Programme auf den Geräten einer Administrationsgruppe installieren. Kaspersky Security Center Cloud Console bietet eine Richtlinie für jedes Kaspersky-Programm 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 ein Kaspersky-Programm aktiv sein. Geräte wenden die Einstellungswerte einer aktiven Richtlinie für ein Kaspersky-Programm 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 ein einzelnes Programm 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 Virenepidemien 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 lokale Programmeinstellungen 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 Security Center Cloud Console, *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 eines Programms für alle Geräte gesetzt werden, die zu einer Gruppe gehören.

Die Einstellungswerte, die eine Richtlinie vorgibt, lassen sich für einzelne Geräte mit lokalen Programmeinstellungen 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 das Programm 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 das Programm den lokalen Einstellungswert auf jedem Client-Gerät und nicht den Wert, der in der Richtlinie angegeben ist. Der Einstellungswert kann dabei über die lokalen Programmeinstellungen geändert werden.

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

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

- Durch die Gruppenrichtlinie, wenn die Änderung der Einstellung gesperrt wurde.

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

Lizenzierung des Programms

Dieser Abschnitt enthält Informationen zur Lizenzierung des Programms.

Lizenzierung von Kaspersky Security Center Cloud Console: Szenario

Nach diesem Szenario können Sie die Kaspersky Security Center Cloud Console und verwaltete Sicherheitsanwendungen im Rahmen einer Lizenz verwenden.

Kaspersky Security Center Cloud Console ermöglicht eine zentrale Verteilung von Lizenzschlüsseln für Kaspersky-Programme auf Client-Geräte sowie die Überwachung der Schlüsselverwendung und die Verlängerung der Gültigkeitsdauer der Lizenz.

Wenn Sie die Kaspersky Security Center Cloud Console 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 Security Center Cloud Console vor dem Erwerb einer Lizenz

Sie können die Kaspersky Security Center Cloud Console zunächst kostenlos testen. Erstellen Sie dazu einen Test-Arbeitsbereich, 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.

Sie können später nicht vom Testmodus in den kommerziellen Modus wechseln. Jeder Testarbeitsbereich wird mit seinem gesamten Inhalt nach 30 Tagen automatisch gelöscht.

Schritte

Das Szenario verläuft in den folgenden Schritten:

1. **Abrufen eines Aktivierungscodes für die Lizenzierung der Kaspersky Security Center Cloud Console im kommerziellen Modus. Erwerb einer Lizenz (oder mehrerer Lizenzen)**

   Unterschiedliche Lizenzen ermöglichen die Nutzung verschiedener Programme 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console für MSPs.

2. **Aktivierung der Kaspersky Security Center Cloud Console beim Erstellen des Arbeitsbereichs**

   Beim Erstellen eines Arbeitsbereichs geben Sie Ihren Lizenzschlüssel an, um Kaspersky Security Center Cloud Console zu aktivieren.

   Wenn Sie über mehrere Lizenzschlüssel verfügen, geben Sie einen davon an – später müssen Sie weitere Lizenzschlüssel in der Kaspersky Security Center Cloud Console hinzufügen, um verwaltete Kaspersky-Programme 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 Ihren Lizenzschlüssel (oder Ihre Lizenzschlüssel) nacheinander der Datenverwaltung des Administrationsservers von Kaspersky Security Center Cloud Console 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 das installierte Kaspersky-Programm lokal mithilfe der Tools der Programmoberfläche aktivieren. Weitere Informationen finden Sie in der Dokumentation zum installierten Programm.

5. **Feststellen, auf welchen Geräten die verwalteten Programme von Kaspersky 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 bald ablaufen:

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

Informationen über den Testmodus von Kaspersky Security Center Cloud Console

Der *Testmodus* ist ein spezieller Modus von Kaspersky Security Center Cloud Console, in dem sich der Benutzer mit den Funktionen von Kaspersky Security Center Cloud Console vertraut machen soll. In diesem Modus können Sie Aktivitäten in einem Arbeitsbereich ausführen, der nur 30 Tage lang gültig ist. Der Testmodus wird direkt nach dem Anlegen eines Test-Arbeitsbereiches aktiviert. Der im Testmodus verfügbare Funktionsumfang entspricht dem, der unter einer Standardlizenz für Kaspersky Endpoint Security for Business Advanced zur Verfügung steht.

In Kaspersky Security Center Cloud Console muss der Administrationsserver nicht lizenziert werden, da Funktionen, die eine spezielle Lizenz benötigen nicht angezeigt werden. Wenn Sie Kaspersky Security Center Cloud Console im Testmodus verwenden möchten, erhalten Sie beim Erstellen Ihres ersten Arbeitsbereichs automatisch eine Testlizenz.

Sie können später nicht vom Testmodus in den kommerziellen Modus wechseln. Jeder Testarbeitsbereich wird mit seinem gesamten Inhalt nach 30 Tagen automatisch gelöscht.

Für die Verwendung der Funktionen von Kaspersky Security Center Cloud Console im Testmodus gelten folgende Einschränkungen:

- Sie können keine Administrationsserver-Hierarchie erstellen. Es können keine virtuellen Administrationsserver erstellt werden.
- Der Bereich **Lizenzverwaltung** ist schreibgeschützt. In diesem Abschnitt können keine Aktionen, einschließlich des Hinzufügens und Entfernens von Lizenzschlüsseln, ausgeführt 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. Virenausbruchsereignisse 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 von Administrationsservern vom lokalen Modus in den Cloud Console-Modus wird nicht unterstützt.
- Statistische KSN-Informationen von Komponenten des Administrationsservers, wie Administrationsserver oder Administrationsagent, werden nicht an Kaspersky gesendet.

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 Kaspersky Security Center Cloud Console im Testmodus

Typ der Einschränkung	Wert
Richtlinien	8
Aufgaben	17
Lizenzschlüssel	1
Installationspakete	5
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	20

Den Kaspersky Marketplace zum Suchen von Kaspersky-Unternehmenslösungen verwenden

Der **Marketplace** ist ein Abschnitt im Hauptmenü, in dem Sie sich das gesamte Angebot an Unternehmenslösungen von Kaspersky anzeigen lassen können, die gewünschten auswählen und anschließend mit dem Kauf auf der Kaspersky-Website fortfahren können. Sie können Filter verwenden, um sich nur die Lösungen anzeigen zu lassen, die zu Ihrem Unternehmen und zu den Anforderungen an Ihr System für Informationssicherheit passen. Wenn Sie eine Lösung auswählen, leitet Sie Kaspersky Security Center Cloud Console 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. Wechseln 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 Security Center Cloud Console 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 Security Center Cloud Console 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

Die Maximalanzahl an Geräten pro Arbeitsbereich beträgt 25.000. Wenn Sie mehr als 10.000 Geräte schützen möchten, müssen Sie einen separaten Arbeitsbereich erstellen. Um dies zu tun, senden Sie eine Anfrage an den Technischen Support von Kaspersky. Diese Anfrage muss die folgenden Informationen enthalten:

- **Benutzer-E-Mail** – Die E-Mail-Adresse des in der Kaspersky Security Center Cloud Console registrierten Benutzers. Dem Benutzer werden Administratorberechtigungen für den erstellten Arbeitsbereich gewährt.

  Nach der Erstellung eines Benutzerkontos in Kaspersky Security Center Cloud Console müssen Sie kein Unternehmen registrieren oder ein Arbeitsbereich für dieses anlegen. Machen Sie in der Anfrage Angeben zu dem Unternehmen und dem Arbeitsbereich.

- **Name des Unternehmens** – Der Name des Unternehmens, in dem Sie Kaspersky Security Center Cloud Console verwenden möchten.

- **Land des Unternehmens** – Das Land, in dem sich das Unternehmen befindet.
- **Name des Arbeitsbereichs** – Der Name des Arbeitsbereichs, der für das Unternehmen angelegt werden soll.
- **Geschätzte Anzahl an Endpunkten** – Die Gesamtanzahl aller Client-Geräte (einschließlich mobiler Geräte), die Sie in dem neuen Arbeitsbereich schützen möchten.
- **Land des Arbeitsbereichs** – Das Land, in dem sich Ihr neuer Arbeitsbereich befinden soll. Diese Einstellung hat Auswirkung auf die Auswahl des Rechenzentrums für die Speicherung des Arbeitsbereichs.

  Beachten Sie, dass Sie bei der Auswahl des Standorts des Arbeitsbereichs für die Länder USA oder Kanada den Bundesstaat oder die Provinz zur Bestimmung des Datencenters angeben müssen.

  Die Werte für **Land des Unternehmens** und **Land des Arbeitsbereichs** können übereinstimmen.
- **Aktivierungscode** – Der Aktivierungscode, den Sie nach dem Erwerb von Kaspersky Security Center Cloud Console erhalten. Stellen Sie sicher, dass die von Ihnen gewünschte Lizenz alle Client-Geräte abdeckt, die geschützt werden sollen.

Nachdem Sie die Anfrage abgeschickt haben, registrieren die Spezialisten von Kaspersky das angegebene Unternehmen und legen für dieses einen Arbeitsbereich an. Wenn das Anlegen des Arbeitsbereichs abgeschlossen ist, erhalten Sie eine Benachrichtigung per E-Mail. Sie können sich mit Ihrem Benutzerkonto an Kaspersky Security Center Cloud Console anmelden und das Ergebnis begutachten.

Ereignisse bei Überschreitung der Lizenzbeschränkung

Kaspersky Security Center Cloud Console ermöglicht das automatische Empfangen von Informationen über Ereignisse bei Überschreitung der Lizenzbeschränkung von Kaspersky-Programmen, 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

Jedes der auf den verwalteten Geräten installierten Kaspersky-Programme 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-Programme 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-Programme nicht nur über einen aktiven Lizenzschlüssel, sondern auch über einen Reserve-Lizenzschlüssel verfügen. Kaspersky-Programme 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 zur Datenverwaltung des Administrationsservers hinzufügen

Beim Hinzufügen eines Lizenzschlüssels über Kaspersky Security Center Cloud Console 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. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Lizenzierung** → **Lizenzen für Kaspersky-Software**.
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 Security Center Cloud Console ermöglicht die Verteilung von Lizenzschlüsseln auf Client-Geräte mit der Aufgabe zur *Verteilung von Lizenzschlüsseln*.

Fügen Sie vor der Bereitstellung einen Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzu.

Um einen Lizenzschlüssel auf Client-Geräte zu verteilen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Wählen Sie das Programm aus, für das Sie einen Lizenzschlüssel hinzufügen möchten.

4. Wählen Sie in der Liste **Aufgabentyp** die Option **Lizenzschlüssel hinzufügen** aus.

5. Folgen Sie den Anweisungen des Assistenten.

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 die Schaltfläche **Erstellen**.

   Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.

8. Um die Aufgabe auszuführen, wählen Sie diese in der Aufgabenliste aus und klicken Sie auf **Starten**.

Bei Ausführung der Aufgabe wird der Lizenzschlüssel auf den ausgewählten Geräten bereitgestellt.

Lizenzschlüssel automatisch verteilen

Kaspersky Security Center Cloud Console 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** → **Lizenzierung** → **Lizenzen für Kaspersky-Software**.

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.

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 Test-Lizenzschlüssel verfügen, wird Ihr Test-Lizenzschlüssel 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 → Lizenzierung → Lizenzen für Kaspersky-Software**.

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 → Lizenzierung → Lizenzen für Kaspersky-Software**.
2. Klicken Sie auf den Namen des gewünschten Lizenzschlüssels.

Im Eigenschaftenfenster des Lizenzschlüssels können Sie Folgendes ansehen:

- Auf der Registerkarte **Allgemein**: die wichtigsten Informationen über den Lizenzschlüssel
- Auf der Registerkarte **Geräte**: die Liste mit Client-Geräten, auf denen der Lizenzschlüssel für die Aktivierung der installierten Kaspersky-Anwendung verwendet wurde

Informationen zu den Lizenzschlüsseln für ein bestimmtes Kaspersky-Programm anzeigen

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

1. Wechseln Sie im Hauptmenü zu **Geräte → Verwaltete Geräte**.

   Wenn das Gerät zur Gruppe nicht zugeordneter Geräte gehört, wechseln Sie stattdessen zu **Gerätesuche und Softwareverteilung → Nicht zugeordnete Geräte**.
2. Klicken Sie auf den Namen des gewünschten Geräts.
3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts den Abschnitt **Programme** 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 aus der Datenverwaltung löschen

Sie können einen Lizenzschlüssel aus der Datenverwaltung des Administrationsservers löschen. Beachten Sie, dass Kaspersky Security Center Cloud Console in folgenden Fällen Ihren Arbeitsbereich automatisch nach 90 Tagen löscht:

- Sie löschen 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 Security Center Cloud Console verwalten. Außerdem verlieren Sie unwiderruflich alle Daten von Kaspersky Security Center Cloud Console. Bei Bedarf können Sie Ihren Arbeitsbereich manuell löschen. Andernfalls empfehlen wir, mindestens einen Lizenzschlüssel in der Datenverwaltung des Administrationsservers aufzubewahren.

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

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

So löschen Sie einen Lizenzschlüssel aus der Datenverwaltung des Administrationsservers:

1. Prüfen Sie, dass der von Ihnen zu löschende Lizenzschlüssel nicht vom Administrationsserver verwendet wird. Wenn der Administrationsserver den Schlüssel verwendet, können Sie ihn nicht löschen. So können Sie dies prüfen:

   a. Klicken Sie im Hauptmenü auf das Einstellungen-Symbol ( ) neben dem Administrationsserver.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

   b. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Lizenzschlüssel** aus.

   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 gelöschte 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** → **Lizenzierung** → **Lizenzen für Kaspersky-Software**.

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 löschen**. Dies bedeutet, dass Sie sich darüber im Klaren sind, dass nach der Löschung des letzten Lizenzschlüssels ebenso der Arbeitsbereich gelöscht wird und die Kontrolle über die verwalteten Geräte verloren geht. Klicken Sie anschließend auf die Schaltfläche **Löschen**.

Infolge dessen wird der ausgewählte Lizenzschlüssel aus der Datenverwaltung gelöscht.

Sie können einen gelöschten Lizenzschlüssel erneut hinzufügen oder einen neuen Schlüssel hinzufügen. Wenn Sie den letzten Lizenzschlüssel gelöscht haben, können Sie ebenfalls einen Lizenzschlüssel hinzufügen, solange der Arbeitsbereich noch nicht gelöscht wurde. Kaspersky Security Center Cloud Console 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 ein Kaspersky-Programm installiert, aber nicht aktiviert ist (z. B. aufgrund einer fehlenden oder abgelaufenen Lizenz).

So zeigen Sie die Geräte an, auf denen sich ein nicht aktiviertes Kaspersky-Programm befindet:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Aufgaben**.

   Die Aufgabenliste wird angezeigt.

2. Klicken Sie auf den Namen der Updateaufgabe für das betreffende Kaspersky-Programm.

   Das Fenster mit den Aufgabeneigenschaften enthält mehrere benannte Registerkarten.

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

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

4. Sortieren Sie die Spalte **Gerät**.

   In der Spalte **Gerät** 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 jedes verwaltete Kaspersky-Programm 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-Programme:

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** 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 das Kaspersky-Programm 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 Programme von Kaspersky verlängern

Lizenzen für Kaspersky-Programme, 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 Security Center Cloud Console Ihren Arbeitsbereich automatisch nach 90 Tagen. Infolgedessen können Sie den Schutz Ihres Netzwerks nicht mehr mit Kaspersky Security Center Cloud Console verwalten. Außerdem verlieren Sie unwiderruflich alle Daten von Kaspersky Security Center Cloud Console. 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 → Lizenzierung → Lizenzen für Kaspersky-Software**.

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

Es öffnet sich das Fenster **Lizenzen für Kaspersky-Software**, in dem Sie 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 Security Center Cloud Console werden die Benachrichtigungen für eine ablaufende Lizenz entsprechend des folgenden Zeitplans angezeigt:

- 30 Tage vor Ablauf
- 7 Tage vor Ablauf
- 3 Tage vor Ablauf
- 24 Stunden vor Ablauf
- Wenn eine Lizenz abgelaufen ist

Kaspersky Security Center Cloud Console nach Ablauf der Lizenz verwenden

Nach Ablauf der Lizenz kann Ihnen Kaspersky die weitere uneingeschränkte Nutzung der Kaspersky Security Center Cloud Console für bis zu 90 Tage gewähren. Während dieses Zeitraums werden der Administrationsserver, der Administrationsagent und die Web-Oberfläche von Kaspersky Security Center Cloud Console ohne Einschränkungen ausgeführt. Kaspersky Security Center Cloud Console 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 Security Center Cloud Console Ihren Arbeitsbereich automatisch. Wenn Sie den Arbeitsbereich behalten möchten, müssen Sie mindestens einen abgelaufenen Lizenzschlüssel verlängern oder einen neuen Lizenzschlüssel zur Datenverwaltung hinzufügen.

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.

Über KSN

Das Kaspersky Security Network (KSN) ist eine Infrastruktur von Online-Diensten, die Zugriff auf die aktuelle Wissensdatenbank von Kaspersky bietet, in der Informationen über die Reputation der Dateien, Web-Ressourcen und Programme enthalten sind. Die Nutzung der Daten aus dem Kaspersky Security Network gewährleistet eine höhere Reaktionsschnelligkeit der Kaspersky-Programme auf Bedrohungen, erhöht die Effektivität vieler Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen. 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-Programme, die von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console, ob auf die KSN-Server erreichbar sind. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet das Programm öffentliche DNS-Server. Dies ist notwendig, um sicherzustellen, dass das Sicherheitsniveau für die verwalteten Geräte beibehalten wird.

Vom Administrationsserver verwaltete Client-Geräte interagieren mithilfe des KSN-Proxyservers mit KSN. Der KSN-Proxyserver bietet folgende Möglichkeiten:

- Client-Geräte können Anfragen an KSN initiieren 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN-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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN-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 das Einstellungen-Symbol ( ) neben dem 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 Security Center Cloud Console 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 entscheiden Sie sich anschließend durch Anklicken einer 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 in den Eigenschaften des Administrationsservers jederzeit 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` läuft.

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.

Lizenzdefinitionen

Dieser Abschnitt enthält Definitionen von Konzepten zur Lizenzierung von Kaspersky-Programmen, die mittels Kaspersky Security Center Cloud Console verwaltet werden.

Über die Lizenz

Eine *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für ein Programm, das Ihnen gemäß den Bedingungen des Endbenutzer-Lizenzvertrags überlassen wird.

Eine Lizenz berechtigt Sie zur Nutzung folgender Leistungen:

- Nutzung des Programms gemäß den Bestimmungen des Endbenutzer-Lizenzvertrags.
- Erhalt von technischem Support.

Der Umfang der Leistungen und die Laufzeit hängen vom Typ der Lizenz ab, anhand derer das Programm aktiviert wurde.

Es sind folgende Lizenztypen vorgesehen:

- *Test*. Eine kostenlose Lizenz zum Kennenlernen des Programms.

  Eine Testlizenz verfügt in der Regel über eine kurze Gültigkeitsdauer. Nachdem die Gültigkeit der Testlizenz abgelaufen ist, stellt Kaspersky Security Center Cloud Console die Funktion ein. Um das Programm weiter nutzen zu können, müssen Sie eine kommerzielle Lizenz erwerben.

  Das Programm kann nur ein einziges Mal mit einer Testlizenz aktiviert werden.

- *Kommerziell.* Eine kostenpflichtige Lizenz, die beim Kauf des Programms zur Verfügung gestellt wird.

  Wenn die kommerzielle Lizenz abläuft, werden wichtige Programmfunktionen deaktiviert. Zur weiteren Nutzung von Kaspersky Security Center Cloud Console ist eine Verlängerung der kommerziellen Lizenz erforderlich. Wenn eine Verlängerung Ihrer Lizenz nicht vorgesehen ist, müssen Sie das Programm von Ihrem Computer entfernen.

Es wird empfohlen, die Gültigkeitsdauer der Lizenz vor deren Ablaufdatum zu verlängern, um einen optimalen 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:

- Lizenzschlüssel oder Bestellnummer
- Informationen über den Benutzer, dem die Lizenz ausgestellt wird
- Informationen über das Programm, das mit der ausgestellten Lizenz aktiviert werden kann
- Maximale Anzahl von Lizenzeinheiten (z. B. Geräte, auf denen das Programm 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 das Programm aktivieren können, um es 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 des Programms 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 Testlizenz kann als aktiver Lizenzschlüssel hinzugefügt werden. Der Lizenzschlüssel für eine Testlizenz 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 Security Center Cloud Console aktiviert. Sie erhalten den Aktivierungscode an die von Ihnen angegebene E-Mail-Adresse, nachdem Sie Kaspersky Security Center Cloud Console erworben haben oder eine Testversion von Kaspersky Security Center Cloud Console bestellt haben.

Zur Aktivierung des Programms mithilfe eines Aktivierungscodes ist ein Internetzugang erforderlich, um sich mit den Aktivierungsservern von Kaspersky zu verbinden. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet das Programm öffentliche DNS-Server.

Wenn das Programm mithilfe eines Aktivierungscodes aktiviert wurde, sendet das Programm in einigen Fällen nach der Aktivierung regelmäßige Anfragen an die Aktivierungsserver von Kaspersky zur Überprüfung des aktuellen Lizenzschlüsselstatus. Zum Versenden von Anfragen benötigt das Programm einen Internetzugang.

Wenn Sie Ihren Aktivierungscode nach der Installation des Programms verloren haben, wenden Sie sich an den Kaspersky-Partner, von dem Sie die Lizenz erworben haben.

Sie können keine Schlüsseldateien zum Aktivieren verwalteter Programme verwenden. Es werden nur Aktivierungscodes akzeptiert.

Über das Abonnement

Ein *Abonnement für Kaspersky Security Center Cloud Console* ist eine Bestellung des Programms mit bestimmten Einstellungen (Ablaufdatum des Abonnements, Anzahl der geschützten Geräte). Ein Abonnement für Kaspersky Security Center Cloud Console kann bei einem Lieferanten von Dienstleistungen abgeschlossen werden (z. B. bei einem Internet-Provider). Das Abonnement kann manuell oder automatisch verlängert oder auch gekündigt werden.

Ein Abonnement kann beschränkt (z. B. auf ein Jahr) oder unbeschränkt (ohne Ablaufdatum) sein. Um Kaspersky Security Center Cloud Console weiterhin zu nutzen, muss ein beschränktes Abonnement rechtzeitig verlängert werden. Ein unbeschränktes Abonnement wird automatisch verlängert, falls der vereinbarte Betrag rechtzeitig an den Dienstleister überwiesen wird.

Nach Ablauf eines befristeten Abonnements wird möglicherweise eine Nachfrist zur Abonnement-Verlängerung gewährt, innerhalb dieser die Funktionalität der Anwendung erhalten bleibt. Verfügbarkeit und Dauer der Nachfrist werden vom Lieferanten der Dienstleistungen bestimmt.

Um Kaspersky Security Center Cloud Console mit einem Abonnement zu nutzen, muss der Aktivierungscode übernommen werden, den Sie von Ihrem Provider erhalten.

Sie können nur dann einen anderen Aktivierungscode für die Nutzung von Kaspersky Security Center Cloud Console verwenden, wenn das Abonnement zuvor abgelaufen ist oder gekündigt wurde.

Für die Abonnement-Verwaltung stehen je nach Provider unterschiedliche Optionen zur Verfügung. Der Provider stellt möglicherweise keine Nachfrist für die Verlängerung des Abonnements zur Verfügung, innerhalb der die Funktionen der Anwendung erhalten bleiben.

Die für ein Abonnement erhaltenen Aktivierungscodes können nicht für die Aktivierung vorheriger Versionen von Kaspersky Security Center Cloud Console verwendet werden.

Bei einer Nutzung des Programms im Abonnement stellt Kaspersky Security Center Cloud Console zum festgelegten Zeitpunkt vor Ablauf des Abonnements automatisch eine Verbindung zum Aktivierungsserver her. Wenn der Zugriff auf den Server mithilfe des System-DNS nicht möglich ist, verwendet das Programm öffentliche DNS-Server. Sie können Ihr Abonnement auf der Website des Dienstanbieters verlängern.

Bereitstellung von Daten

Mit der Kaspersky Security Center Cloud Console kann der Benutzer die Geräte (und die Gerätebesitzer), die mit der Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Software-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 Security Center Cloud Console

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, Unternehmens-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 Security Center Cloud Console übertragen werden

Durch folgen der Links in der Verwaltungskonsole oder der Kaspersky Security Center Cloud Console stimmt der Nutzer zu, die folgenden Daten automatisch zu übertragen:

- Lokalisierung der Kaspersky Security Center Cloud Console
- 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, die für die Funktionsfähigkeit des Arbeitsbereichs erforderlich sind

Kaspersky Security Center Cloud Console verarbeitet die folgenden Daten:

1. Informationen zu den im Netzwerk der Organisation erkannten Geräten

Der Administrationsagent erhält die nachstehend aufgeführten Daten von den im Netzwerk befindlichen Geräten und übermittelt sie an den Administrationsserver:

a. Technische Spezifikationen des erkannten Geräts und seiner Komponenten, die für die Geräteidentifikation erforderlich sind und die mittels Netzwerkabfrage empfangen wurden:

- Active Directory-Abfrage:

  Geräte im Active Directory: an das Gerät vergebener Name; vom Domänencontroller erhaltener Name der Windows-Domäne; Gerätename in der Windows-Umgebung; DNS-Domäne und DNS-Name des Geräts; SAM-Konto (Security Account Manager - Name zur Anmeldung am System, der für die Unterstützung von Clients und Servern, auf denen frühere Versionen des Betriebssystems ausgeführt werden, verwendet wird: z. B. Windows NT 4.0, Windows 95, Windows 98 und LAN Manager); an die Domäne vergebener Name; vergebene Namen an die Gruppen, zu denen das Gerät gehört; vergebener Name an den Benutzer, der das Gerät verwaltet; weltweit eindeutige ID (GUID - Global Unique Identifier) und übergeordnete GUID des Gerät

  Während der Abfrage des Active Directory-Netzwerks werden die folgenden Datenarten verarbeitet, um Informationen über die verwaltete Infrastruktur anzuzeigen, und um dem Benutzer diese Information verwenden zu lassen, beispielsweise für die Bereitstellung des Schutzes:

- Active Directory-Organisationseinheiten: an die Organisationseinheit vergebener Name; an die Domäne vergebener Name; GUID der Organisationseinheit und GUID der übergeordneten Einheit.

- Active Directory-Domänen: vom Domänencontroller empfangener Name der Windows-Domäne; DNS-Domäne; GUID der Domäne.

- Active Directory-Benutzer: Anzeigename des Benutzers; an den Nutzer vergebener Name; an die Domäne vergebener Name; an die Organisation des Benutzers vergebener Name; an die Abteilung, in welcher der Benutzer beschäftigt ist, vergebener Name; an den Benutzer, der als Manager des Benutzers agiert, vergebener Name; vollständiger Name des Benutzers; SAM-Konto (Security Account Manager); E-Mail-Adresse; alternative E-Mail-Adresse; Haupttelefonnummer; alternative Telefonnummer; Handynummer; Name der Position des Benutzers; an die Gruppen, zu denen der Benutzer gehört, vergebene Namen; Benutzer-GUID; User Security Identifier (SID) (eindeutiger Binärwert zur Identifizierung des Benutzers als Sicherheitsprinzipal); User Principal Name (UPN) – Anmeldename im Internetstil für einen Benutzer, der auf dem Internetstandard RFC 822 basiert. Der UPN ist kürzer als der eindeutige Name und einfacher zu merken. Grundsätzlich ist der UPN der E-Mail-Adresse des Benutzers zugeordnet.

- Active Directory-Gruppen: an die Gruppe vergebener Name; E-Mail-Adresse; an die Domäne vergebener Name; SAM-Konto (Security Account Manager); an die weiteren Gruppen, zu denen die Gruppe gehört; vergebene Namen; Benutzer-SID; Gruppen-GUID.

b. Abfrage der Windows-Domäne:

- Name der Windows-Domäne oder -Arbeitsgruppe

- Name des NetBIOS des Geräts

- DNS-Domäne und DNS-Name des Geräts

- Name und Beschreibung des Geräts

- Sichtbarkeit des Geräts im Netzwerk

- IP-Adresse des Geräts

- Gerätetyp (Workstation, Server, SQL-Server, Domänencontroller usw.)

- Betriebssystem-Typ des Geräts
- Version des Betriebssystems des Geräts
- Zeitpunkt der letzten Aktualisierung der Geräteinformationen
- Zeitpunkt der letzten Sichtbarkeit des Geräts im Netzwerk

c. Abfrage des IP-Bereichs:

- IP-Adresse des Geräts
- DNS-Name oder NetBIOS-Name des Geräts
- Name und Beschreibung des Geräts
- MAC-Adresse des Geräts
- Zeitpunkt der letzten Sichtbarkeit des Geräts im Netzwerk

2. Einzelheiten zu den verwalteten Geräten

Der Administrationsagent übermittelt die unten aufgeführten Daten von dem Gerät an den Administrationsserver. Der Benutzer gibt den Anzeigenamen und die Beschreibung des Geräts in die Schnittstelle der Kaspersky Security Center Cloud Console ein:

a. Technische Spezifikationen des verwalteten Geräts und seiner Komponenten, die zur Identifizierung des Geräts benötigt werden, einschließlich:

- Anzeigename (anhand des NetBIOS-Namens erzeugt, kann manuell geändert werden) und Beschreibung des Geräts (manuell eingegeben)
- Name und Typ der Windows-Domäne (Windows NT-Domäne / Windows-Arbeitsgruppe)
- Gerätename in der Windows-Umgebung
- DNS-Domäne und DNS-Name des Geräts
- IP-Adresse des Geräts
- Subnetzmaske des Geräts
- Standort des Gerätenetzwerks
- MAC-Adresse des Geräts
- Betriebssystem-Typ des Geräts
- Ob das Gerät eine virtuelle Maschine zusammen mit einem Hypervisor ist
- Ob das Gerät eine dynamische virtuelle Maschine als Teil einer Virtual Desktop Infrastructure (VDI) ist
- Geräte-GUID
- Instanz-ID des Administrationsagenten
- Installations-ID des Administrationsagenten

- Permanente ID des Administrationsagenten

b. Sonstige Spezifikationen verwalteter Geräte und ihrer Komponenten, die für die Prüfung verwalteter Geräte und für das Treffen von Entscheidungen darüber, ob spezifische Patches und Updates zutreffen, erforderlich sind:

- Status des Windows Update-Agenten (WUA)
- Architektur des Betriebssystems
- Anbieter des Betriebssystems
- Versionsnummer des Betriebssystems
- Versions-ID des Betriebssystems
- Zielordner des Betriebssystems
- Der Typ der virtuellen Maschine, wenn das Gerät eine virtuelle Maschine ist
- Wartezeit auf eine Geräteantwort
- Ob der Administrationsagent im Standalone-Modus läuft

c. Detaillierte Informationen zur Aktivität auf verwalteten Geräten:

- Datum und Uhrzeit des letzten Updates
- Datum und Uhrzeit der letzten Sichtbarkeit des Geräts im Netzwerk
- Neustart-Wartestatus ("Neustart ist erforderlich.")
- Zeit, in der das Gerät eingeschaltet war

d. Einzelheiten zu den Benutzerkonten des Geräts und ihren Arbeitssitzungen

e. Statistiken zum Betrieb der Verteilungspunkte, wenn das Gerät ein Verteilungspunkt ist:

- Datum und Uhrzeit der Erstellung des Verteilungspunkts
- Name des Arbeitsordners
- Größe des Arbeitsordners
- Anzahl der Synchronisierungen mit dem Administrationsserver
- Datum und Uhrzeit der letzten Synchronisierung des Geräts mit dem Administrationsserver
- Anzahl und Gesamtgröße der übertragenen Dateien
- Anzahl und Gesamtgröße der von Kunden heruntergeladenen Dateien
- Von Kunden mittels Transmission Control Protocol (TCP) heruntergeladenes Datenvolumen
- An Kunden mit Multicasting gesendetes Datenvolumen

- Von Kunden mittels Multicasting heruntergeladenes Datenvolumen
- Anzahl der Multicast-Verteilungen
- Gesamtvolumen der Multicast-Verteilungen
- Anzahl der Synchronisierungen mit Clients nach der letzten Synchronisierung mit dem Administrationsserver

f. Name des virtuellen Administrationsservers, der das Gerät verwaltet

g. Informationen zu Cloud-Geräten:

- Cloud-Region
- Virtual Private Cloud (VPC)
- Cloud Availability Zone (Verfügbarkeitszone)
- Cloud-Subnetz
- Cloud-Placement-Gruppe

h. Einzelheiten zu den mobilen Geräten. Das verwaltete Programm überträgt diese Daten vom mobilen Gerät an den Administrationsserver. Die vollständige Liste der Daten ist in der Dokumentation des verwalteten Programms verfügbar.

3. Einzelheiten zu den auf dem Gerät installierten Anwendungen von Kaspersky.

Die verwaltete Anwendung überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver:

a. Verwaltete Anwendungen von Kaspersky und Komponenten von Kaspersky Security Center Cloud Console, die auf dem Gerät installiert sind

b. Einstellungen der auf dem verwalteten Gerät installierten Kaspersky-Programme:

- Name und Version des Programms von Kaspersky
- Status
- Status des Echtzeitschutzes
- Datum und Uhrzeit der letzten Untersuchung des Geräts
- Anzahl der erkannten Bedrohungen
- Anzahl der nicht desinfizierten Objekte
- Aufgaben für die Kaspersky-Sicherheitsanwendung
- Verfügbarkeit und Status der Komponenten des Programms
- Zeitpunkt des letzten Updates und Version der Antiviren-Datenbanken
- Einzelheiten zu den Einstellungen des Kaspersky-Programms

- Informationen zu aktiven Lizenzschlüsseln
- Informationen zu Reserve-Lizenzschlüsseln
- Datum der Programminstallation
- ID der Programminstallation

c. Statistiken zum Programmbetrieb: Ereignisse in Bezug auf Statusänderungen von Komponenten des Kaspersky-Programms auf dem verwalteten Gerät und Ereignisse in Bezug auf die Ausführung von Aufgaben, die von den Anwendungskomponenten initiiert wurden

d. Durch das Kaspersky-Programm definierter Gerätestatus

e. Von dem Kaspersky-Programm zugeordnete Tags

f. Installierte und anwendbare Updates für das Kaspersky-Programm:

- Anzeigename, Version und Sprache des Programms
- Interner Name des Programms
- Programmname und -version aus dem Registrierungsschlüssel
- Ordner der Programminstallation
- Patch-Version
- Liste der installierten Autopatches für das Programm
- Ob das Programm vom Kaspersky Security Center Cloud Console unterstützt wird
- Ob das Programm auf einem Cluster installiert ist

g. Details zu Fehlern der Datenverschlüsselung auf Geräten: Fehler-ID, Zeitpunkt des Auftretens, Operationstyp (Verschlüsselung/Entschlüsselung), Fehlerbeschreibung, Dateipfad, Beschreibung der Verschlüsselungsregel, Geräte-ID und Benutzername

4. Ereignisse der Komponenten der Kaspersky Security Center Cloud Console und verwalteten Kaspersky-Anwendungen.

   Der Administrationsagent übermittelt Daten von dem Gerät an den Administrationsserver.

   Die Beschreibung eines Ereignisses kann die folgenden Daten enthalten:

   a. Gerätename

   b. Name des Benutzers des Geräts

   c. Name des Administrators, der das Gerät per Fernzugriff verbunden hat

   d. Name, Version und Anbieter des auf dem Gerät installierten Programms

   e. Pfad zum auf dem Gerät befindlichen Ordner der Programminstallation

   f. Pfad zur Datei auf dem Gerät und Dateiname

   g. Programmname und Befehlszeilenparameter, unter denen das Programm ausgeführt wurde

h. Patchname, Name der Patchdatei, Patch-ID, Grad der durch das Patch behobenen Schwachstelle, Beschreibung des Patch-Installationsfehlers

i. IP-Adresse des Geräts

j. MAC-Adresse des Geräts

k. Neustartstatus des Geräts

l. Name der Aufgabe, die das Ereignis bekanntgegeben hat

m. Ob das Gerät auf Standalone-Modus umgestellt wurde und der Grund für die Umstellung

n. Informationen über den Vorfall auf dem Gerät: Art des Vorfalls, Name des Vorfalls, Signifikanz, Beschreibung des Vorfalls, von dem Kaspersky-Programm übermittelte Einzelheiten zum Vorfall

o. Größe des freien Festplattenspeichers auf dem Gerät

p. Ob das Kaspersky-Programm im eingeschränkten Funktionsmodus ausgeführt wird, IDs der Funktionsbereiche

q. Alter und neuer Wert der Einstellung des Kaspersky-Programms

r. Beschreibung des Fehlers, der auftrat, als das Kaspersky-Programm oder eine seiner Komponenten den Betrieb ausführte

5. Einstellungen der Komponenten der Kaspersky Security Center Cloud Console und des verwalteten Kaspersky-Programms in Richtlinien und Richtlinienprofilen.

   Der Benutzer gibt Daten in die Schnittstelle der Kaspersky Security Center Cloud Console ein.

6. Aufgabeneinstellungen der Komponenten der Kaspersky Security Center Cloud Console und verwalteten Kaspersky-Programme

   Der Benutzer gibt Daten in die Schnittstelle der Kaspersky Security Center Cloud Console ein.

7. Von der Funktion "Schwachstellen- und Patch-Management" verarbeitete Daten.

   Der Administrationsagent übermittelt die unten aufgeführten Daten von dem Gerät an den Administrationsserver:

   a. Einzelheiten zu auf verwalteten Geräten installierten Anwendungen und Patches (Programm-Registry). Anwendungen können anhand von Informationen zu ausführbaren Dateien identifiziert werden, die von der Funktion zur Programmkontrolle auf verwalteten Geräten erkannt wurden:

      - ID der Anwendung/des Patches
      - ID der übergeordneten Anwendung (für einen Patch)
      - Name und Version der Anwendung/des Patches
      - Ob die Anwendung/der Patch eine .msi-Datei des Windows-Installers ist
      - Anbieter der Anwendung/des Patches
      - ID der Lokalisierungssprache
      - Installationsdatum der Anwendung/des Patches

- Pfad der Anwendungsinstallation
- Website des technischen Supports des Herstellers der Anwendung/des Patches
- Telefonnummer für den technischen Support
- ID der installierten Anwendungsinstanz
- Kommentar
- Deinstallationsschlüssel
- Schlüssel für die Installation im Silent-Modus
- Patch-Klassifizierung
- Webadresse für weitere Informationen zum Patch
- Registrierungsschlüssel der Anwendung
- Versionsnummer der Anwendung
- Benutzer-SID
- Betriebssystemtyp (Windows, Unix)

b. Informationen zur auf verwalteten Geräten erkannten Hardware (Hardware-Register):

- Geräte-ID
- Gerätetyp (Hauptplatine, CPU, RAM, Massenspeichergerät, Grafikkarte, Soundkarte, Netzwerkschnittstellen-Controller, Monitor, optisches Laufwerk)
- Gerätename
- Beschreibung
- Anbieter
- Seriennummer
- Version
- Informationen zum Treiber: Entwickler, Version, Beschreibung und Freigabedatum
- Informationen zum BIOS: Entwickler, Version, Seriennummer und Freigabedatum
- Chipset
- Taktfrequenz
- Anzahl der CPU-Kerne
- Anzahl der CPU-Threads
- CPU-Plattform

- Rotationsgeschwindigkeit des Speichergeräts
- Typ des Arbeitsspeichers, Teilenummer
- Videospeicher
- Soundkarten-Codec

c. Einzelheiten zu in Drittsoftware auf verwalteten Geräten erkannten Schwachstellen:

- Kennung der Schwachstelle
- Signifikanz der Schwachstelle (Warnung, Hoch, Kritisch)
- Typ der Schwachstelle (Microsoft, Drittanbieter)
- Webadresse der Seite, auf der die Schwachstelle beschrieben ist
- Zeitpunkt der Erstellung des Schwachstelleneintrags
- Name des Anbieters
- Lokalisierter Name des Herstellers
- Anbieter-ID
- Name der Anwendung
- Lokalisierter Name der Anwendung
- Installationscode der Anwendung
- Anwendungsversion
- Lokalisierungssprache der Anwendung
- Liste der CVE-Kennungen aus der Schwachstellenbeschreibung
- Die Schwachstellen blockierenden Schutztechnologien von Kaspersky (Schutz vor bedrohlichen Dateien, Verhaltensanalyse, Schutz vor Web-Bedrohungen, Schutz vor E-Mail-Bedrohungen, Programm-Überwachung, ZETA Shield)
- Pfad zur Objektdatei, in der die Schwachstelle erkannt wurde
- Zeit der Erkennung der Schwachstelle
- IDs der Artikel der Wissensdatenbank aus der Schwachstellenbeschreibung
- IDs der Sicherheits-Bulletins aus der Schwachstellenbeschreibung
- Liste der Updates für die Schwachstelle
- Ob ein Exploit für die Schwachstelle existiert
- Ob Schadsoftware für die Schwachstelle existiert

d. Einzelheiten zu Updates, die für auf verwalteten Geräten installierte Dritthersteller-Anwendungen zur Verfügung stehen:

- Name und Version der Anwendung
- Anbieter
- Lokalisierungssprache der Anwendung
- Betriebssystem
- Liste der Patches gemäß der Installationsreihenfolge
- Originalversion der Anwendung, auf die das Patch angewandt wird
- Anwendungsversion nach der Patch-Installation
- Patch-ID
- Versionsnummer
- Installationskennzeichnungen
- Endbenutzer-Lizenzverträge für den Patch
- Ob der Patch eine Voraussetzung zur Installation anderer Patches ist
- Lite der erforderlichen installierten Anwendungen und ihrer Updates
- Informationsquellen zum Patch
- Weitere Informationen über den Patch (Adressen von Webseiten)
- Webadresse für den Patch-Download, Dateiname, Version, Revision und SHA-256

e. Informationen zu Microsoft-Updates, die von der WSUS-Funktion gefunden wurden:

- Update-Revisions-Nummer
- Microsoft-Update-Typ (Treiber, Anwendung, Kategorie, Detectoid)
- Update-Ereigniskategorie gemäß dem Bulletin Microsoft Security Response Center (MSRC) (niedrig, mittel, hoch, kritisch)
- IDs des das Update betreffenden MSRC-Bulletins
- IDs von Artikeln in der MSRC-Wissensdatenbank
- Update-Name (Header)
- Update-Beschreibung
- Ob das Update-Installationsprogramm interaktiv ist
- Installationskennzeichnungen

- Update-Klassifizierung (kritische Updates, Definitionsupdates, Treiber, Funktionspaket, Sicherheits-Updates, Service Pack, Tools, Update-Rollups, Updates, Upgrade)
- Informationen zu der Anwendung, auf die das Update angewandt wird
- ID des Endbenutzer-Lizenzvertrags (EULA)
- EULA-Text
- Ob der EULA für die Update-Installation zugestimmt werden muss
- Informationen über die dazugehörigen Updates (ID und Revisionsnummer)
- Update-ID (globale Microsoft-Windows-Update-Identität)
- IDs für ersetzte Updates
- Ob das Update verborgen ist
- Ob das Update erforderlich ist
- Installationsstatus zum Update (Nicht zutreffend, Nicht zur Installation zugewiesen, Zugewiesen, Installation wird ausgeführt, Installiert, Fehlgeschlagen, Neustart ist erforderlich, Nicht zur Installation zugewiesen (neue Version))
- CVE-IDs für das Update
- Das Unternehmen, welches das Update herausgegeben hat, oder der Wert "Kein Unternehmen vorhanden"

f. Liste der Microsoft-Updates, die von der WSUS-Funktion gefunden wurden und die auf dem Gerät installiert werden müssen.

8. Informationen über ausführbare Dateien, die von der Funktion "Programmkontrolle" auf verwalteten Geräte erkannt wurden (können mit Informationen aus der Programm-Registry verbunden sein). Eine vollständige Liste der Daten ist dem Abschnitt zu entnehmen, der die Daten für Geräte beschreibt, die durch das jeweilige Programm verwaltet werden.

   Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver.

9. Informationen über in das Backup aufgenommene Dateien. Eine vollständige Liste der Daten ist dem Abschnitt zu entnehmen, der die Daten für Geräte beschreibt, die durch das jeweilige Programm verwaltet werden.

   Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver.

10. Informationen über Dateien, die von Spezialisten von Kaspersky für eine detaillierte Analyse angefordert wurden. Eine vollständige Liste der Daten ist dem Abschnitt zu entnehmen, der die Daten für Geräte beschreibt, die durch das jeweilige Programm verwaltet werden.

    Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver.

11. Informationen über den Status und die Auslösung von Regeln für die Adaptive Kontrolle von Anomalien. Eine vollständige Liste der Daten ist dem Abschnitt zu entnehmen, der die Daten für Geräte beschreibt, die durch das jeweilige Programm verwaltet werden.

    Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver.

12. Informationen über Geräte (Speichereinheiten, Tool zur Informationsübertragung, Informations-Hardcopy-Tools und Verbindungsbusse), die auf dem verwalteten Gerät installiert oder mit diesem verbunden sind und von der Funktion "Gerätekontrolle" erkannt wurden. Eine vollständige Liste der Daten ist dem Abschnitt zu entnehmen, der die Daten für Geräte beschreibt, die durch das jeweilige Programm verwaltet werden.

    Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver.

13. Daten über Alarme:

    - Datum und Uhrzeit des ersten Telemetrie-Ereignisses des Alarms
    - Datum und Uhrzeit des letzten Telemetrie-Ereignisses des Alarms
    - Name der auslösenden Regel (wird vom Benutzer in der Benutzeroberfläche von Kaspersky Security Center Cloud Console angegeben)
    - Status des Alarms
    - Auflösung (Fehlalarm, Echter Alarm, Niedrige Priorität)
    - ID und Name des Benutzers, dem der Alarm zugewiesen ist
    - Individuelle ID in der Datenbank von Kaspersky Security Center Cloud Console und der Name des Geräts, das mit den als Alarmquelle geltenden Ereignissen in Verbindung steht
    - SID und Name des Benutzers des Geräts, das mit den als Alarmquelle geltenden Ereignissen in Verbindung steht
    - Charakteristiken, die mit den als Alarmquelle geltenden Ereignissen in Verbindung stehen:
        - IP-Adresse
        - MD5-Hash der Datei sowie ihr Dateipfad
        - Webadresse
        - Domäne
    - Weitere Informationen zum Objekt, das mit dem Alarm in Verbindung steht (vom Programm empfangen)
    - Kommentare zu dem Alarm:
        - Datum und Uhrzeit des Hinzufügens des Kommentars
        - Benutzer, der den Kommentar hinzugefügt hat
        - Text des Kommentars
    - Änderungsverlauf für den Alarm:
        - Datum und Uhrzeit der ersten Änderung
        - Benutzer, der die Änderung ausgeführt hat
        - Beschreibung der Änderung

14. Daten über Vorfälle:

    - Datum und Uhrzeit des ersten Ereignisses des Vorfalls
    - Datum und Uhrzeit des letzten Ereignisses des Vorfalls
    - Name des Vorfalls (vom Benutzer in der Benutzeroberfläche von Kaspersky Security Center Cloud Console angegeben)
    - Kurzbeschreibung des Vorfalls
    - Priorität des Vorfalls
    - Status des Vorfalls
    - ID und Name des Benutzers, dem der Vorfall zugewiesen wurde
    - Auflösung (Fehlalarm, Echter Alarm, Niedrige Priorität, Zusammengeführt)
    - Kommentar zu dem Vorfall:
        - Datum und Uhrzeit des Hinzufügens des Kommentars
        - Benutzer, der den Kommentar hinzugefügt hat
        - Text des Kommentars
    - Änderungsprotokoll für den Vorfall:
        - Datum und Uhrzeit der ersten Änderung
        - Benutzer, der die Änderung ausgeführt hat
        - Beschreibung der Änderung

15. Durch die Funktion zur Datenverschlüsselung von Kaspersky-Programmen verarbeitete Daten.

    Das verwaltete Programm überträgt die unten aufgeführten Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Der Benutzer gibt die Beschreibung des Laufwerks in die Schnittstelle der Kaspersky Security Center Cloud Console ein:

    a. Liste der Laufwerke auf den Geräten:

        - Laufwerkname
        - Verschlüsselungsstatus
        - Laufwerkart (Bootlaufwerk, Festplatte)
        - Seriennummer des Laufwerks
        - Beschreibung

    b. Informationen zu Fehlern bei der Datenverschlüsselung auf den Geräten:

        - Datum und Zeitpunkt, zu dem der Fehler auftrat

- Vorgangsart (Verschlüsselung, Entschlüsselung)
- Fehlerbeschreibung
- Dateipfad
- Regelbeschreibung
- Geräte-ID
- Benutzername
- Fehler-ID

c. Einstellungen zur Datenverschlüsselung von dem Kaspersky-Programm.

Eine vollständige Liste der Daten ist dem Abschnitt zu entnehmen, der die Daten für Geräte beschreibt, die durch das jeweilige Programm verwaltet werden.

16. Einzelheiten zu den eingegebenen Aktivierungscodes.

Der Benutzer gibt Daten in die Schnittstelle der Kaspersky Security Center Cloud Console ein.

17. Benutzerkonten.

Der Benutzer gibt die unten aufgeführten Daten in die Schnittstelle der Kaspersky Security Center Cloud Console ein:

a. Name

b. Beschreibung

c. Vollständiger Name

d. E-Mail-Adresse

e. Erste Telefonnummer

f. Passwort

18. Daten für die Authentifizierung des Benutzers mittels Active Directory:

a. Einstellungen der Active Directory Federation Services (ADFS):

- Haupt-URL des Authentifizierungsanbieters
- Vertrauenswürdige Root-Zertifikate für ADFS
- Die in ADFS generierte Client-ID
- Geheimer Schlüssel zum Schutz des Zugriffs auf ADFS
- Gültigkeitsbereich der Token
- Domäne der Active Directory, in welcher die Integration stattfindet
- Name des Token-Felds mit der Benutzer-SID

- Name des Token-Felds mit dem Array der Benutzergruppen-SIDs

Der Benutzer gibt Daten in die Schnittstelle der Kaspersky Security Center Cloud Console ein.

b. Daten, die Kaspersky Security Center Cloud Console automatisch vom ADFS-Server erhält:

- Aussteller (issuer)
- Autorisierungsendpunkt des Benutzers (authorization_endpoint)
- Token-Endpunkt (token_endpoint)
- JSON Web Key Set URI (jwks_uri)
- Aussteller des Zugriffstokens (access_token_issuer)
- Benutzerinformationsendpunkt (userinfo_endpoint)
- Endpunkt der Sessionbeendigung (end_session_endpoint)
- Zertifikate zum Signieren der Tokens

19. Revisionsverlauf der verwalteten Objekte: Administrationsserver, Administrationsgruppe, Richtlinie, Aufgabe, Benutzer / Sicherheitsgruppe, Installationspaket.

    Der Benutzer gibt die unten aufgeführten Daten in die Schnittstelle der Kaspersky Security Center Cloud Console ein:

    a. Administrationsserver

    b. Administrationsgruppe

    c. Richtlinie

    d. Aufgabe

    e. Benutzer / Sicherheitsgruppe

    f. Installationspaket

20. Register der gelöschten Managementobjekte.

    Der Benutzer gibt Daten in die Schnittstelle der Kaspersky Security Center Cloud Console ein.

21. Aus der Datei erzeugte Installationspakete wie auch Installationseinstellungen.

    Der Benutzer gibt Daten in die Schnittstelle der Kaspersky Security Center Cloud Console ein.

22. Daten, die für die Anzeige der Mitteilungen von Kaspersky in der Kaspersky Security Center Cloud Console erforderlich sind:

    a. Informationen zu verwalteten Kaspersky-Programmen, die vom Benutzer verwendet werden: Anwendungs-ID, vollständige Versionsnummer.

    b. Die vom Benutzer verwendete Lokalisation der Benutzeroberfläche von Kaspersky Security Center Cloud Console.

c. Informationen zur Aktivierung des Programms auf dem Gerät: Softwarelizenz-ID; Laufzeit der Softwarelizenz; Ablaufdatum und -uhrzeit der Softwarelizenz; Art der verwendeten Softwarelizenz; Art des Software-Abonnements; Ablaufdatum und -uhrzeit des Software-Abonnements; aktueller Status des Software-Abonnements; Grund des aktuellen/sich ändernden Status des Software-Abonnements; ID des Eintrags in der Preisliste, über welche die Softwarelizenz erworben wurde.

d. Informationen zur rechtlichen Vereinbarung, die der Benutzer bei der Nutzung der Software akzeptiert: Art der rechtlichen Vereinbarung; Fassung der rechtlichen Vereinbarung; Parameter, der angibt, ob der Benutzer die Bedingungen der rechtlichen Vereinbarung akzeptiert hat.

e. Informationen zu den vom Rechteinhaber erhaltenen Mitteilungen: ID der Mitteilung; Zeitpunkt des Eingangs der Mitteilung; Empfangsstatus der Mitteilung.

Der Benutzer gibt Daten in die Schnittstelle der Kaspersky Security Center Cloud Console ein.

23. Benutzereinstellungen der Kaspersky Security Center Cloud Console.

    Der Benutzer gibt die unten aufgeführten Daten in die Schnittstelle der Kaspersky Security Center Cloud Console ein:

    a. Lokalisierungssprache der Benutzeroberfläche

    b. Farbschema der Benutzeroberfläche

    c. Anzeigeneinstellungen der Überwachungsleiste

    d. Informationen zum Status von Benachrichtigungen: Bereits gelesen/Noch nicht gelesen

    e. Status von Spalten in Tabellen: Einblenden/Ausblenden

    f. Tutorial-Fortschritt

24. Daten, die der Benutzer in die Schnittstelle der Kaspersky Security Center Cloud Console eingibt:

    a. Name der Administrationsgruppe bei der Erstellung einer Administrationsgruppen-Hierarchie

    b. E-Mail-Adresse bei der Konfigurierung von E-Mail-Benachrichtigungen

    c. Tags für Geräte und Tagging-Regeln

    d. Tags für Anwendungen

    e. Benutzerkategorien der Anwendungen

    f. Rollenname bei der Zuweisung einer Rolle zu einem Benutzer

    g. Informationen über Subnetze: Name des Subnetzes, Beschreibung, Adresse und Maske

    h. Einstellungen für Berichte und Wahlmöglichkeiten

    i. Alle anderen von dem Benutzer eingegebenen Daten

25. Daten, die von einem lokal bereitgestellten sekundären Administrationsserver erhalten wurden.

    Die vom Kaspersky Security Center Administrationsserver verarbeiteten Daten sind in der Online-Hilfe von Kaspersky Security Center beschrieben.

Bei der Verbindung eines lokal bereitgestellten Kaspersky Security Center Administrationsservers als sekundären Administrationsserver in Bezug auf die Kaspersky Security Center Cloud Console verarbeitet die Kaspersky Security Center Cloud Console die folgenden Datenarten aus dem sekundären Administrationsserver:

a. Informationen über die Geräte im Netzwerk der Organisation, die infolge der Gerätesuche im Active Directory-Netzwerk oder Windows-Netzwerk oder über den Scan von IP-Intervallen erhalten wurden

b. Informationen über die organisatorischen Einheiten des Active Directory, Domänen, Benutzer und Gruppen, die infolge einer Active Directory-Netzwerkabfrage erhalten wurden

c. Informationen über verwaltete Geräte, ihre technischen Spezifikationen, einschließlich der für die Geräteidentifikation erforderlichen Spezifikationen, Konten von Gerätebenutzern und ihre Arbeitssitzungen

d. Informationen über mobile Geräte, die mittels des Exchange ActiveSync-Protokolls übertragen werden

e. Informationen über mobile Geräte, die mittels des iOS MDM-Protokolls übertragen werden

f. Einzelheiten zu den auf dem Gerät installierten Anwendungen von Kaspersky: Einstellungen, Betriebsstatistiken, durch die Anwendung definierter Gerätestatus, installierte und anwendbare Updates, Tags

g. Mit Ereigniseinstellungen aus Komponenten des Kaspersky Security Centers und der verwalteten Kaspersky-Programme übertragene Informationen

h. Einstellungen der Komponenten von Kaspersky Security Center und der verwalteten Kaspersky-Programme in Richtlinien und Richtlinienprofilen

i. Aufgabeneinstellungen der Komponenten von Kaspersky Security Center und verwalteten Kaspersky-Programme

j. Von der Funktion "Schwachstellen- und Patch-Management" verarbeitete Daten: Einzelheiten zu Anwendungen und Patches; Informationen über die Hardware: Einzelheiten zu in Drittsoftware auf verwalteten Geräten erkannten Schwachstellen; Einzelheiten zu für Dritthersteller-Anwendungen verfügbaren Updates; Einzelheiten zu von der WSUS-Funktion gefundenen Microsoft-Updates

k. Benutzerkategorien der Anwendungen

l. Einzelheiten zu ausführbaren Dateien, die von der Funktion "Programmkontrolle" auf verwalteten Geräten gefunden wurden

m. Einzelheiten zu Dateien, die in das Backup aufgenommenen wurden

n. Einzelheiten zu Dateien, die in die Quarantäne aufgenommenen wurden

o. Einzelheiten zu Dateien, die von Spezialisten von Kaspersky für eine detaillierte Analyse angefordert wurden

p. Informationen über den Status und die Auslösung von Regeln für die Adaptive Kontrolle von Anomalien

q. Einzelheiten zu Geräten (Speichereinheiten, Tool zur Informationsübertragung, Informations-Hardcopy-Tools und Verbindungsbusse), die auf dem verwalteten Gerät installiert oder mit diesem verbunden sind und von der Funktion "Programmkontrolle" erkannt wurden

r. Verschlüsselungseinstellungen des Kaspersky-Programms: Verzeichnis der Chiffrierschlüssel, Status der Geräteverschlüsselung

s. Informationen über Fehler der Datenverschlüsselung, die auf den Geräten mittels der Datenverschlüsselungsfunktion von Kaspersky-Programmen durchgeführt wurde

t. Liste der verwalteten programmierbaren Logikcontroller (PLCs)

u. Einzelheiten zu den eingegebenen Aktivierungscodes

v. Benutzerkonten

w. Revisionsverlauf von Managementobjekten

x. Register der gelöschten Managementobjekte

y. Aus der Datei erstellte Installationspakete sowie Installationseinstellungen

z. Benutzereinstellungen der Kaspersky Security Center Web Console

aa. Alle Daten, die der Benutzer in die Verwaltungskonsole oder die Schnittstelle der Kaspersky Security Center Cloud Console eingibt

ab. Zertifikat für eine sichere Verbindung verwalteter Geräte mit den Komponenten von Kaspersky Security Center

26. Aus dem verwalteten Gerät bei der Nutzung der Funktion "Ferndiagnose" hochgeladene Informationen: Diagnosedateien (Dump-Datei, Protokolldateien, Log-Dateien etc.) und in diesen Dateien enthaltene Daten.

27. Daten, die für die Integration von Kaspersky Security Center Cloud Console in ein SIEM-System zum Ereignisexport benötigt werden:

    - Daten, die für die Verbindung und Authentifizierung benötigt werden:

        - Adresse und Port für die Verbindung des SIEM-Systems

        - Authentifizierungszertifikat des SIEM-Servers

        - Vertrauenswürdiges Zertifikat und privater Schlüssel für die Client-Authentifizierung von Kaspersky Security Center Cloud Console in dem SIEM-System

      Der Benutzer gibt Daten in die Schnittstelle der Kaspersky Security Center Cloud Console ein.

    - Daten, die durch Kaspersky Security Center Cloud Console vom SIEM-System empfangen werden: öffentlicher Schlüssel des SIEM-Serverzertifikats zur Authentifizierung des SIEM-Servers.

28. Daten, die von Kaspersky Security Center Cloud Console für die Interaktion mit der Cloud-Umgebung benötigt werden:

    a. Amazon Web Services (AWS):

        - ID des Zugriffsschlüssels des IAM-Benutzerkontos

        - Geheimer Schlüssel des IAM-Benutzerkontos

    b. Microsoft Azure:

        - Azure Anwendungs-ID

- Azure-Abonnement-ID
- Azure-App-Kennwort
- Benutzerkonto-Name zum Azure-Repository
- Zugriffsschlüssel des Benutzerkontos zum Azure-Repository

c. Google Cloud:

- Google-Client-E-Mail
- Projekt-ID
- Privater Schlüssel

Der Benutzer gibt Daten in die Schnittstelle der Kaspersky Security Center Cloud Console ein.

29. Von einem nicht unterstützten Kaspersky-Programm übertragene Daten

    Wenn Sie den Administrationsagenten auf einem Gerät installieren, auf dem ein Kaspersky -Programm installiert ist, das jedoch nicht von Kaspersky Security Center Cloud Console unterstützt wird, überträgt dieses Kaspersky -Programm dennoch Daten an Kaspersky Security Center Cloud Console (Die Liste der Daten finden Sie im Abschnitt "Über die Bereitstellung von Daten" im Hilfesystem des Programms.). Kaspersky Security Center Cloud Console kann die Daten, die von einem nicht unterstützten Programm übertragen werden, jedoch nicht in der Art verarbeiten, wie der Prozess für die wichtigsten Funktionen von Kaspersky Security Center Cloud Console beschrieben ist.

    Die Liste der unterstützten Kaspersky-Programme wird in der Online-Hilfe von Kaspersky Security Center Cloud Console angezeigt.

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 Security für Windows Server
- Kaspersky Security für mobile Endgeräte
- Kaspersky Embedded Systems Security für Windows
- Kaspersky Embedded Systems Security für Linux

Die Liste der verarbeiteten Daten ist unter https://ksc.kaspersky.com/home/legaldocuments?locale=de in der Vereinbarung zur Datenverarbeitung zu Kaspersky Security Center Cloud Console veröffentlicht. Suchen Sie auf der Webseite für Rechtsdokumente den Textblock mit dem Namen "Vereinbarung zur Kaspersky Security Center Cloud Console" und scrollen Sie im Textblock nach unten zum Abschnitt mit den Daten für Geräte, die durch das entsprechende Programm verwaltet werden. Sie können zu diesem Zweck auch die Standard-Suchfunktion Ihres Browsers verwenden.

Lokal verarbeitete Daten

Die einzige Komponente von Kaspersky Security Center, die lokal in einer Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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.

Zusätzliche Verarbeiter personenbezogener Daten

Neben Kaspersky gibt es für die Kaspersky Security Center Cloud Console die folgenden Verarbeiter für personenbezogene Daten mit Bezug auf den Arbeitsbereich.

Name und Anschrift der Organisation:
Microsoft Ireland Operations Limited
One Microsoft Place, South County Business Park, Leopardstown
Dublin 18 D18 P521

Dienst:
Microsoft Azure (Datenhosting)

Die Länder, in denen die Daten verarbeitet werden, sind im Abschnitt Auswahl der Rechenzentren für die Speicherung der Informationen in Kaspersky Security Center Cloud Console aufgelistet.

Über die rechtlichen Dokumente für Kaspersky Security Center Cloud Console

Um Kaspersky Security Center Cloud Console verwenden zu können, müssen Sie Ihre Zustimmung zu den Bestimmungen und Bedingungen der auf der Website von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console anmelden, um einen Arbeitsbereich zu verwalten. Sie können die Vereinbarung der Kaspersky Security Center Cloud Console und die Vereinbarung zur Datenverarbeitung von Kaspersky Security Center Cloud Console lesen, wenn Sie einen Unternehmensarbeitsbereich erstellen.

Bitte lesen Sie sich die Texte aller rechtlichen Dokumente sorgfältig durch, bevor Sie mit der Verwendung von Kaspersky Security Center Cloud Console beginnen.

Endbenutzer-Lizenzvertrag für Kaspersky-Programme

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-Programme nutzen dürfen.

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

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

Sie können jederzeit Ihre Akzeptanz des Endbenutzer-Lizenzvertrags widerrufen.

Wenn Sie den Endbenutzer-Lizenzvertrag eines Kaspersky-Programms nicht akzeptieren, können Sie dieses Programm nicht verwenden.

Härtungsleitfaden

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

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

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

Der Härtungsleitfaden enthält Empfehlungen und Funktionen zur Konfiguration von Kaspersky Security Center Cloud Console und ihren Komponenten, mit dem Ziel, das Risiko einer Kompromittierung zu verringern.

Der Härtungsleitfaden enthält die folgenden Informationen:

- Konfiguration der Benutzerkonten in Kaspersky Security Center Cloud Console
- 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 Security Center Cloud Console beginnen, werden Sie dazu aufgefordert, die Kurzversion des Härtungsleitfadens zu lesen.

Beachten Sie, dass Sie Kaspersky Security Center Cloud Console erst verwenden können, nachdem Sie bestätigt haben, dass Sie den Härtungsleitfaden gelesen haben.

So können Sie den Härtungsleitfaden lesen:

1. Öffnen Sie die Kaspersky Security Center Cloud Console und melden Sie sich an. Kaspersky Security Center Cloud Console 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 anzeigen**.

3. Nachdem Sie den Härtungsleitfaden gelesen haben, aktivieren Sie das Kontrollkästchen **Ich bestätige, dass ich den Härtungsleifaden vollständig gelesen habe und ihn verstehe** und klicken Sie anschließend auf die Schaltfläche **Akzeptieren**.

Sie können die Kaspersky Security Center Cloud Console jetzt verwenden.

Wenn eine neue Version des Härtungsleitfadens veröffentlicht wird, werden Sie von Kaspersky Security Center Cloud Console dazu aufgefordert, diese zu lesen.

Kaspersky Security Center Cloud Console-Architektur

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

In der Anfangsphase der Architekturentwurfs empfehlen wir, sich mit den Komponenten von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console
- 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 Security Center Cloud Console

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 Security Center Cloud Console zu erhöhen. Wenn diese Funktion aktiviert ist, müssen Sie jedes Mal, wenn Sie sich mit E-Mail-Adresse und Kennwort an der Kaspersky Security Center Cloud Console anmelden, einen zusätzlichen 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).

Wir raten dringend davon ab, die Authenticator-App auf demselben Gerät zu installieren, von dem aus die Verbindung zur Kaspersky Security Center Cloud Console hergestellt wird. Sie können eine Authenticator-App auf Ihrem Mobilgerät installieren.

Verbieten der Speicherung des Administratorpassworts

Wenn Sie Kaspersky Security Center Cloud Console 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 einen vorkonfigurierten Satz an Rechten für die Administration der Kaspersky Security Center Cloud Console verwenden.

Zugriffsrechte auf Programmfunktionen konfigurieren

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

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 Software von Drittanbietern 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-Software und Kaspersky-Programmen 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 Security Center Cloud Console 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 ein Kennwort beispielsweise für Kaspersky Endpoint Security für Windows, Kaspersky Security für Windows Server, den Administrationsagenten und weitere Kaspersky-Anwendungen festlegen. Nachdem Sie den Kennwortschutz aktiviert haben, empfehlen wir, diese Einstellungen zu sperren, indem Sie das "Schloss" schließen.

Verwenden von Kaspersky Security Network

Wir empfehlen, in allen Richtlinien der verwalteten Anwendungen und in den Eigenschaften von Kaspersky Security Center Cloud Console die Verwendung von Kaspersky Security Network (KSN) zu aktivieren und die KSN-Erklärung zu akzeptieren. Wenn Sie Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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.

Erstkonfiguration von Kaspersky Security Center Cloud Console

Dieser Abschnitt beschreibt das Hauptszenario für die Bereitstellung von Kaspersky Security Center Cloud Console, 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:

- Beginnen der Arbeiten mit einem Arbeitsbereich als Administrator Ihres Unternehmens
- Ermitteln der Geräte in Ihrem Netzwerk (Bei Bedarf weisen Sie Verteilungspunkte zu und installieren Programmpakete manuell auf den Verteilungspunkten)
- Bereitstellung verwalteter Kaspersky-Programme auf den Client-Geräten und die Konfiguration der Tools, die dem Netzwerkschutz, der Überwachung und der regelmäßigen Aktualisierung der Kaspersky-Datenbanken, -Programm-Module und -Programme dienen

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

Erforderliche Vorrausetzungen

Vor dem Start:

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

Schritte

Die Konfiguration der Kaspersky Security Center Cloud Console 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. **Erstellen des Arbeitsbereichs für Ihr Unternehmen**

   Ein Konto erstellen und anschließend einen Arbeitsbereich für Ihr Unternehmen erstellen.

3. **Den Schnellstartassistenten ausführen**

Öffnen Sie Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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.

   Wenn Sie Kaspersky Security für Windows Server bereitstellen, vergewissern Sie sich, dass die Programmdatenbanken aktuell sind.

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-Programme 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.

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. **Aktualisierung von Programmen von Drittanbietern und Behebung von Schwachstellen in Programmen von Drittanbietern (optional)**

   Kaspersky Security Center Cloud Console 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 Security Center Cloud Console bereitgestellt und konfiguriert ist, können Sie mit der Überwachung des Netzwerkschutzstatus fortfahren.

Arbeitsbereiche verwalten

In diesem Abschnitt wird beschrieben, wie Sie Konten und Arbeitsbereiche in Kaspersky Security Center Cloud Console verwenden können.

Informationen zur Verwaltung von Arbeitsbereichen in Kaspersky Security Center Cloud Console

Mithilfe von Kaspersky Security Center Cloud Console können Sie folgende Aktionen ausführen:

- Konto erstellen.
- Konto bearbeiten.
- Ein Unternehmen registrieren und einen Arbeitsbereich erstellen.
- Informationen zum Unternehmen und zu Arbeitsbereichen bearbeiten.
- Arbeitsbereich und Unternehmen löschen.
- Konto löschen.

Erste Schritte mit Kaspersky Security Center Cloud Console

Dieser Abschnitt enthält Informationen darüber, wie Sie sich bei Kaspersky Security Center Cloud Console registrieren und mit der Verwendung beginnen.

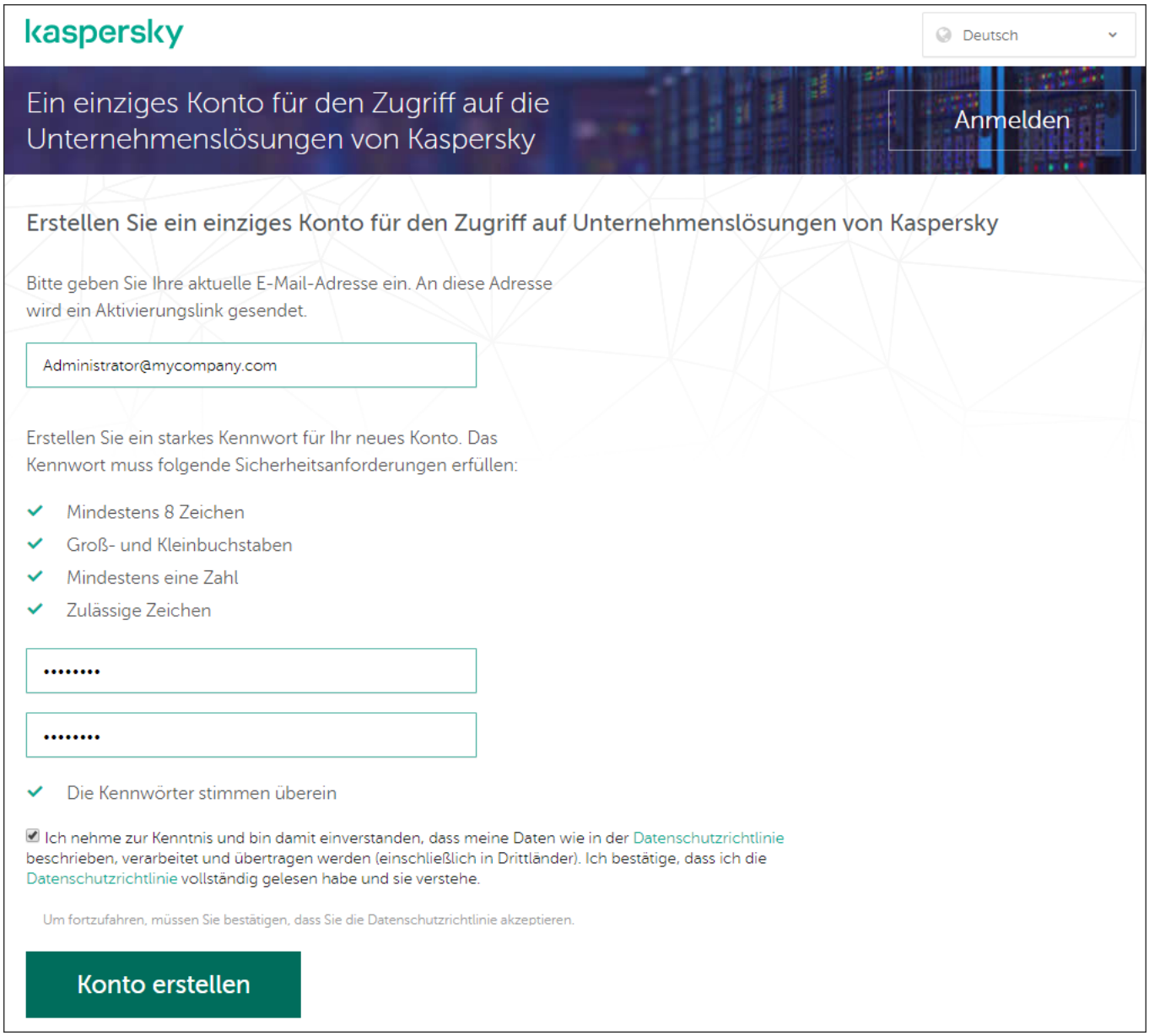
Die Anmeldung an der Kaspersky Security Center Cloud Console umfasst folgende Schritte:

1. Ein Konto erstellen und bestätigen.
2. Ein Unternehmen registrieren und einen Arbeitsbereich erstellen.

Ein Benutzerkonto erstellen

So erstellen Sie ein Benutzerkonto in Kaspersky Security Center Cloud Console:

1. Wechseln Sie in Ihrem Browser zur Kaspersky Security Center Cloud Console.
2. Klicken Sie auf der Startseite der Kaspersky Security Center Cloud Console auf die Schaltfläche **Ein Benutzerkonto anlegen**.
3. Geben Sie auf der Seite **Erstellen Sie ein Benutzerkonto für den Zugriff auf die Unternehmenslösungen von Kaspersky** die E-Mail-Adresse, das Kennwort und die Kennwortbestätigung für Ihr Benutzerkonto ein (siehe Abbildung unten).



Erstellung eines Benutzerkontos in Kaspersky Security Center Cloud Console

4. Klicken Sie auf den Link **Datenschutzrichtlinie** und lesen Sie sich den Text der Datenschutzrichtlinie sorgfältig durch.

5. Wenn Sie wissen und damit einverstanden sind, dass Ihre Daten wie in der Datenschutzrichtlinie beschrieben verarbeitet und übermittelt werden (auch an Drittländer), und Sie bestätigen, dass Sie die Datenschutzrichtlinie vollständig gelesen und verstanden haben, aktivieren Sie das Kontrollkästchen neben dem Einwilligungstext zur Datenverarbeitung in Übereinstimmung mit der Datenschutzrichtlinie, und klicken Sie anschließend auf die Schaltfläche **Benutzerkonto anlegen**.

Wenn Sie die Datenschutzrichtlinie nicht akzeptieren, können Sie Kaspersky Security Center Cloud Console nicht verwenden.

Die Schaltfläche wird erst verfügbar, nachdem Sie das Kontrollkästchen aktiviert haben.

Es wird eine Seite angezeigt, auf der Sie aufgefordert werden, Ihre E-Mails zu überprüfen. Von Kaspersky wird eine Nachricht an die von Ihnen angegebene E-Mail-Adresse gesendet. Die Nachricht enthält einen Link, um die Erstellung des Benutzerkontos abzuschließen.

6. Schließen Sie die Seite und öffnen Sie die E-Mail-Nachricht in Ihrem Postfach.

7. Klicken Sie auf den Link in der von Kaspersky gesendeten Nachricht, um zu Ihrer Seite mit Ihrem Benutzerkonto zu gelangen.

8. Klicken Sie auf der Seite **Aktivierung des Benutzerkontos** auf die Schaltfläche **Fortsetzen**, um die Kontoaktivierung abzuschließen.

Die Erstellung des Benutzerkontos in der Kaspersky Security Center Cloud Console ist abgeschlossen.

Registrieren eines Unternehmens und Erstellen eines Arbeitsbereichs

Unmittelbar nach der Erstellung des Kontos können Sie ein Unternehmen registrieren und einen Arbeitsbereich für dieses Unternehmen erstellen.

> Wenn Sie mehr als 10.000 Geräte schützen möchten, müssen Sie nicht wie unten beschreiben, ein Unternehmen registrieren und einen Arbeitsbereich in Kaspersky Security Center Cloud Console anlegen. Stattdessen können Sie eine Anfrage an den Technischen Support von Kaspersky schicken. Machen Sie in der Anfrage Angaben zu Ihrem Unternehmen und den zu erstellenden Arbeitsbereich.

Momentan können Sie nur ein Unternehmen registrieren und einen Arbeitsbereich erstellen. In zukünftigen Versionen von Kaspersky Security Center Cloud Console können Sie zusätzliche Arbeitsbereiche für Ihr Unternehmen erstellen. Dies wird Ihnen helfen, Ihre Unternehmensstruktur auf Arbeitsbereiche abzubilden, indem Sie für jeden Unternehmenszweig einen separaten Arbeitsbereich erstellen.

Bevor Sie anfangen, stellen Sie sicher, dass Ihnen die folgenden Informationen vorliegen:

- Der Name des Unternehmens, in dem Sie die Softwarelösung verwenden möchten.
- Das Land, in dem sich das Unternehmen befindet. Wenn das Unternehmen in den USA oder Kanada befindet, muss Ihnen außerdem der Bundesstaat bzw. die Provinz bekannt sein.
- Die Gesamtanzahl der Computer und der mobilen Geräte des Unternehmens, die Sie schützen möchten.

So registrieren Sie ein Unternehmen und erstellen einen Arbeitsbereich in Kaspersky Security Center Cloud Console:

1. Wechseln Sie in Ihrem Browser zur Kaspersky Security Center Cloud Console.

2. Klicken Sie auf der Startseite von Kaspersky Security Center Cloud Console auf die Schaltfläche **Anmelden**.

3. Geben Sie die E-Mail-Adresse und das Kennwort ein, die Sie bei der Erstellung des Benutzerkontos angegeben haben, und klicken Sie anschließend auf **Anmelden**.

   Der Assistent zum Erstellen eines Arbeitsbereichs wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

4. Auf der Seite **Schritt 01: Nutzungsbedingungen für Kaspersky Security Center Cloud Console** des Assistenten gehen Sie wie folgt vor:

   a. Lesen Sie sorgfältig den Lizenzvertrag, die Datenschutzrichtlinie und die Vereinbarung zur Datenverarbeitung für die Softwarelösung durch.

b. Wenn Sie zusätzlich zu den Bedingungen des Lizenzvertrags und der Vereinbarung zur Datenverarbeitung damit einverstanden sind, dass Ihre Daten gemäß der Beschreibung in der Datenschutzrichtlinie verarbeitet und (auch in Drittländer) übertragen werden, und Sie die Datenschutzrichtlinie vollständig gelesen und verstanden haben, aktivieren Sie das Kontrollkästchen neben den drei aufgeführten Dokumenten und klicken Sie auf die Schaltfläche **Akzeptieren**.

Wenn Sie den Bestimmungen und Bedingungen nicht zustimmen, verwenden Sie Kaspersky Security Center Cloud Console nicht.

Wenn Sie auf **Ablehnen** klicken, wird der Vorgang der Erstellung eines Arbeitsbereichs abgebrochen.

5. Geben Sie auf der Seite **Schritt 02: Informationen zum Unternehmen** des Assistenten allgemeine Informationen zu Ihrem Unternehmen an.

   Füllen Sie die folgenden Felder aus:

   - **Name Ihres Unternehmens** (erforderlich)

     Geben Sie den Namen des Unternehmens an, in dem Sie die Softwarelösung verwenden möchten. Sie können einen Text mit bis zu 255 Zeichen eingeben. Der Text darf Groß- und Kleinbuchstaben, Ziffern, Leerzeichen, Punkte, Kommas, Minuszeichen, Gedankenstriche und Unterstriche enthalten. Der angegebene Name des Unternehmens wird in Kaspersky Security Center Cloud Console angezeigt.

   - Feld **Zusätzliche Unternehmensbeschreibung** (optional)

     Sie können zusätzliche Informationen zum Unternehmen angeben, das Sie registrieren. Sie können einen Text mit bis zu 255 Zeichen eingeben. Der Text darf Groß- und Kleinbuchstaben, Ziffern, Leerzeichen, Punkte, Kommas, Minuszeichen, Gedankenstriche und Unterstriche enthalten.

6. Geben Sie auf der Seite **Schritt 03: Informationen zum Arbeitsbereich** des Assistenten Informationen zum Arbeitsbereich an, den Sie für Ihr Unternehmen erstellen möchten.

   Füllen Sie die folgenden Pflichtfelder aus:

   - **Name des Arbeitsbereichs**. Geben Sie den Namen des Arbeitsbereichs an, in dem Sie die Softwarelösung verwenden möchten. Sie können einen Text mit bis zu 255 Zeichen eingeben. Der Text darf Groß- und Kleinbuchstaben, Ziffern, Leerzeichen, Punkte, Kommas, Minuszeichen, Gedankenstriche und Unterstriche enthalten. Der angegebene Name des Arbeitsbereichs wird in Kaspersky Security Center Cloud Console angezeigt.

   - **Land**. Wählen Sie in der Dropdown-Liste das Land aus, in dem sich der Arbeitsbereich befindet. Wenn Sie USA oder Kanada auswählen, geben Sie in der unter diesem Feld angezeigten Dropdown-Liste **Bundesstaat** auch den Bundesstaat an.

   - **Anzahl der Geräte**. Geben Sie die Gesamtanzahl der Computer und der mobilen Geräte an, die Sie in diesem Arbeitsbereich schützen möchten.

     Im Eingabefeld kann eine Zahl im Bereich von 300 bis 10 000 eingegeben werden.

7. Führen Sie auf der Seite **Schritt 04: Lizenz für neuen Arbeitsbereich** des Assistenten eine der folgenden Aktionen aus:

   - Wenn Sie Kaspersky Security Center Cloud Console ausprobieren möchten, klicken Sie auf den Link **Ich möchte einen Testarbeitsbereich erstellen**.

     Wir empfehlen Ihnen, Ihre eigenen Geräte an Ihren Testarbeitsbereich anzuschließen und alle Änderungen an den Einstellungen zu testen und die Ergebnisse zu notieren.

Sie können einen Testarbeitsbereich nicht durch Eingabe eines Aktivierungscodes in eine kommerzielle Lizenz verwandeln. Um eine kommerzielle Lizenz zu verwenden, müssen Sie den Arbeitsbereich löschen und einen neuen erstellen.

- Wenn Sie Kaspersky Security Center Cloud Console unter einer kommerziellen Lizenz verwenden möchten, geben Sie den Aktivierungscode ein und klicken Sie auf die Schaltfläche **Überprüfen**.

Die Registrierung eines Unternehmens und Erstellung eines Arbeitsbereichs in Kaspersky Security Center Cloud Console ist damit abgeschlossen.

Nach Vorbereitung des Arbeitsbereichs erhalten Sie eine E-Mail-Nachricht mit einem Link zum Arbeitsbereich.

Arbeitsbereich von Kaspersky Security Center Cloud Console öffnen

Direkt nach der Erstellung eines Arbeitsbereichs für Kaspersky Security Center Cloud Console wird der Arbeitsbereich automatisch geöffnet. Später können Sie den Arbeitsbereich wie in diesem Abschnitt beschrieben öffnen.

Wenn Sie ein Administrator eines virtuellen Administrationsservers sind, haben Sie nur Zugriff auf den virtuellen Administrationsserver. Nachdem Sie sich angemeldet und den Arbeitsbereich geöffnet haben, zeigt Ihnen Kaspersky Security Center Cloud Console die Benutzeroberfläche des virtuellen Administrationsservers an. Sie können weder zum primären Administrationsserver noch zu anderen sekundären Administrationsservern wechseln.

Der Administrator eines virtuellen Administrationsservers muss Zugriff auf genau einen virtuellen Administrationsserver haben. Wenn Sie keine Zugriffsrecht für den primären Server, aber für mehrere virtuelle Servern haben, können Sie sich nicht an der Kaspersky Security Center Cloud Console anmelden.

Um den Arbeitsbereich von Kaspersky Security Center Cloud Console zu öffnen, gehen Sie wie folgt vor:

1. Wechseln Sie in Ihrem Browser zur Kaspersky Security Center Cloud Console.
2. Melden Sie sich mit Ihrem Konto bei Kaspersky Security Center Cloud Console an, indem Sie den Benutzernamen und das Kennwort eingeben.
3. Wenn Sie zweistufige Überprüfung eingerichtet haben, geben Sie den Einmal-Sicherheitscode ein, den Sie entweder per SMS erhalten haben oder der in Ihrer Authenticator-App erzeugt wurde (anhängig von der Methode der zweistufigen Überprüfung, die Sie eingerichtet haben).

   Die Seite des Portals zeigt Ihnen das Unternehmen, für welches Sie Administrator sind, und die Liste seiner Arbeitsbereiche an.
4. Klicken Sie auf den Namen des gewünschten Arbeitsbereichs oder auf den Link **Zum Arbeitsbereich wechseln**, um zum Arbeitsbereich zu gelangen.

   Es kann manchmal vorkommen, dass der Arbeitsbereich aufgrund von Wartungsarbeiten unzugänglich ist. In diesem Fall können Sie nicht zum Arbeitsbereich von Kaspersky Security Center Cloud Console wechseln.

   In einen Arbeitsbereich, der zum Löschen markiert ist, kann nicht gewechselt werden.
5. Falls rechtlich verbindliche Dokumente für Kaspersky Security Center Cloud Console geändert wurden, seitdem Sie deren Bedingungen akzeptiert haben, werden auf der Portalseite die geänderten Dokumente angezeigt.

Führen Sie folgende Schritte aus:

a. Lesen Sie die angezeigten Dokumente aufmerksam durch.

b. Wenn Sie die Bedingungen der angezeigten Dokumente annehmen, aktivieren Sie die Kontrollkästchen neben den entsprechenden Dokumenten und klicken Sie anschließend auf die Schaltfläche **Ich akzeptiere die Bedingungen**.

> Wenn Sie die Bedingungen nicht akzeptieren, dürfen Sie die gewählte Softwarelösung von Kaspersky nicht mehr verwenden.

> Wenn Sie auf **Ablehnen** klicken, wird der Vorgang abgebrochen.

Der Arbeitsbereich von Kaspersky Security Center Cloud Console wird geöffnet.

Von Kaspersky Security Center Cloud Console abmelden

Wenn Sie Ihre Arbeit beendet haben, sollten Sie Ihre aktuelle Sitzung sicher beenden, indem Sie sich von der Kaspersky Security Center Cloud Console abmelden.

So melden Sie sich von der Kaspersky Security Center Cloud Console ab:

Wechseln Sie im Hauptmenü zu Ihren Kontoeinstellungen und wählen Sie anschließend **Abmelden.**

Kaspersky Security Center Cloud Console wird beendet und es wird die Anmeldeseite angezeigt. Sie können diese Seite im Browser bei Bedarf schließen. Alle Daten aus Ihrem Arbeitsbereich werden gespeichert.

Verwalten des Unternehmens und der Liste der Arbeitsbereiche

Dieser Abschnitt beschreibt, wie Sie die Unternehmensdaten und die Liste mit Arbeitsbereichen, die in Ihrem Konto in Kaspersky Security Center Cloud Console registriert sind, ansehen, Informationen über das Unternehmen und die Arbeitsbereiche bearbeiten und Arbeitsbereiche und Unternehmen löschen können.

Momentan können Sie nur ein Unternehmen registrieren und einen Arbeitsbereich erstellen. In zukünftigen Versionen von Kaspersky Security Center Cloud Console können Sie zusätzliche Arbeitsbereiche für Ihr Unternehmen erstellen. Dies wird Ihnen helfen, Ihre Unternehmensstruktur auf Arbeitsbereiche abzubilden, indem Sie für jeden Unternehmenszweig einen separaten Arbeitsbereich erstellen.

Informationen über Unternehmen und Arbeitsbereiche bearbeiten

Sie können die Informationen über Unternehmen und Arbeitsbereiche bearbeiten, die Sie beim Hinzufügen des Unternehmens zu Kaspersky Security Center Cloud Console angegeben haben.

So bearbeiten Sie Informationen über Unternehmen und Arbeitsbereiche:

1. Wechseln Sie in Ihrem Browser zur Kaspersky Security Center Cloud Console.

2. Melden Sie sich mit Ihrem Konto bei Kaspersky Security Center Cloud Console an, indem Sie den Benutzernamen und das Kennwort eingeben.

3. Wenn Sie zweistufige Überprüfung eingerichtet haben, geben Sie den Einmal-Sicherheitscode ein, den Sie entweder per SMS erhalten haben oder der in Ihrer Authenticator-App erzeugt wurde (anhängig von der Methode der zweistufigen Überprüfung, die Sie eingerichtet haben).

   Auf der Seite des Portals wird das Unternehmen, in dem Sie über Administratorrechte verfügen, und eine Liste der Arbeitsbereiche angezeigt.

4. Gehen Sie wie folgt vor, wenn Sie den Namen und die Beschreibung des Unternehmens ändern möchten:

   a. Klicken Sie in dem Bereich mit den Unternehmensinformationen auf das Symbol **Bearbeiten** ( ).

   b. Bearbeiten Sie den Namen bzw. die Beschreibung des Unternehmens nach Bedarf.

   c. Klicken Sie auf **Speichern**.

      Um auf die Änderungen zu verzichten, klicken Sie auf die Schaltfläche **Abbrechen**.

5. Gehen Sie wie folgt vor, wenn Sie den Namen des Arbeitsbereichs ändern möchten:

   a. Klicken Sie in dem Bereich mit den Informationen zum Arbeitsbereich auf das Symbol **Bearbeiten** ( ).

   b. Bearbeiten Sie den Namen des Arbeitsbereichs nach Bedarf.

   c. Klicken Sie auf **Speichern**.

      Um auf die Änderungen zu verzichten, klicken Sie auf die Schaltfläche **Abbrechen**.

Die bearbeiteten Informationen werden in Kaspersky Security Center Cloud Console angezeigt.

Löschen eines Arbeitsbereichs und eines Unternehmens

Der Arbeitsbereich eines Unternehmens kann entweder manuell oder automatisch gelöscht werden. Nach der Löschung des letzten Arbeitsbereichs werden auch die Unternehmensdaten automatisch gelöscht.

Manuelle Löschung

Sie können den Arbeitsbereich eines Unternehmens löschen, wenn beschlossen wurde, den Arbeitsbereich nicht länger zu verwenden.

> Nach der Löschung des Arbeitsbereichs verbleiben alle Sicherheitsanwendungen weiterhin auf den verwalteten Geräten. Deshalb wird empfohlen, vor der Löschung des Arbeitsbereichs entweder den Kennwortschutz aller Sicherheitsanwendungen zu entfernen oder die Sicherheitsanwendungen von den verwalteten Geräten zu deinstallieren.

So löschen Sie einen Arbeitsbereich und ein Unternehmen:

1. Wechseln Sie in Ihrem Browser zur Kaspersky Security Center Cloud Console.

2. Melden Sie sich mit Ihrem Konto bei Kaspersky Security Center Cloud Console an, indem Sie den Benutzernamen und das Kennwort eingeben.

3. Wenn Sie zweistufige Überprüfung eingerichtet haben, geben Sie den Einmal-Sicherheitscode ein, den Sie entweder per SMS erhalten haben oder der in Ihrer Authenticator-App erzeugt wurde (anhängig von der Methode der zweistufigen Überprüfung, die Sie eingerichtet haben).

   Auf der Seite des Portals wird das Unternehmen, in dem Sie über Administratorrechte verfügen, und eine Liste der Arbeitsbereiche angezeigt.

4. Wählen Sie den Arbeitsbereich aus, den Sie löschen möchten.

5. Klicken Sie rechts im Abschnitt mit dem ausgewählten Arbeitsbereich auf das Symbol **Löschen** ().

   Das Fenster **Arbeitsbereich löschen** wird geöffnet.

6. Bestätigen Sie im Fenster **Arbeitsbereich löschen** die Löschung des Arbeitsbereichs.

Der Arbeitsbereich wird zum Löschen markiert. Der Block mit Informationen zum Arbeitsbereich wird mit einem roten Rahmen markiert.

Der Block mit den Informationen zum Arbeitsbereich wird zusätzlich im Abschnitt **Zum Löschen ausgewählt** im unteren Bereich der Seite angezeigt.

Es ist nicht möglich, zu einem Arbeitsbereich zu wechseln, der zum Löschen ausgewählt ist, und ihn zu verwalten.

Wenn Sie einen Arbeitsbereich nicht zum Löschen markieren können, wenden Sie sich an den Technischen Support von Kaspersky. Nach dem Empfang der Anfrage werden der Arbeitsbereich und das Unternehmen von einem Techniker des Technischen Supports von Kaspersky gelöscht.

Die zum Löschen markierten Arbeitsbereiche können sich ab dem Datum der Markierung sieben Tage lang in diesem Status befinden. Nach sieben Tagen werden sie automatisch gelöscht.

Während dieses Zeitraums können Sie das Löschen eines Arbeitsbereichs, der entsprechend markiert wurde, erzwingen oder das Löschen des Arbeitsbereichs abbrechen.

Gehen Sie wie folgt vor, um das Löschen eines Arbeitsbereichs zu erzwingen:

1. Wechseln Sie in Ihrem Browser zur Kaspersky Security Center Cloud Console.

2. Melden Sie sich mit Ihrem Konto bei Kaspersky Security Center Cloud Console an, indem Sie den Benutzernamen und das Kennwort eingeben.

3. Wenn Sie zweistufige Überprüfung eingerichtet haben, geben Sie den Einmal-Sicherheitscode ein, den Sie entweder per SMS erhalten haben oder der in Ihrer Authenticator-App erzeugt wurde (anhängig von der Methode der zweistufigen Überprüfung, die Sie eingerichtet haben).

   Auf der Seite des Portals wird das Unternehmen, in dem Sie über Administratorrechte verfügen, und eine Liste der Arbeitsbereiche angezeigt.

4. Klicken Sie im Abschnitt **Zum Löschen ausgewählt** im Block mit Informationen zum Arbeitsbereich auf die Option **Löschen erzwingen**.

   Das Fenster **Arbeitsbereich löschen** wird geöffnet.

5. Geben Sie im Fenster **Arbeitsbereich löschen** die ID des Arbeitsbereichs ein, den Sie löschen möchten.

Die ID des Arbeitsbereichs wird zwecks Bestätigung abgefragt, damit Sie den Arbeitsbereich nicht aus Versehen löschen. Nach dem Löschen des Arbeitsbereichs kann er nicht wiederhergestellt werden.

Die ID des Arbeitsbereichs wird im Block mit Informationen zum Arbeitsbereich unterhalb seines Namens angezeigt.

6. Klicken Sie im Fenster **Arbeitsbereich löschen** auf die Schaltfläche **OK**.

Der Arbeitsbereich wird gelöscht. Alle Daten über Benutzer und verwaltete Geräte werden samt zugehörigen Einstellungen gelöscht.

Automatische Löschung

Kaspersky Security Center Cloud Console löscht einen Arbeitsbereich automatisch nach:

- 30 Tagen, nachdem die Testlizenz abgelaufen ist.
- 90 Tagen, nachdem alle kommerziellen Lizenzen oder Abonnement-Lizenzen in der Datenverwaltung des Administrationsservers abgelaufen sind.
- 90 Tagen, nachdem Sie den letzten, manuell zur Datenverwaltung hinzugefügten, Lizenzschlüssel (aktiv, als Reserve oder nicht verwendet) gelöscht haben.

Kaspersky Security Center Cloud Console benachrichtigt die Administratoren des Arbeitsbereichs 30 Tage, 7 Tage und 1 Tag vor der Löschung.

Löschen eines Arbeitsbereichs widerrufen

Sie können das Löschen eines Arbeitsbereichs, der zum Löschen markiert wurde, abbrechen.

Es ist nicht möglich, das Löschen eines Arbeitsbereichs abzubrechen, der bereits gelöscht wurde.

Gehen Sie wie folgt vor, um das Löschen des Arbeitsbereichs abzubrechen:

1. Wechseln Sie in Ihrem Browser zur Kaspersky Security Center Cloud Console.
2. Melden Sie sich mit Ihrem Konto bei Kaspersky Security Center Cloud Console an, indem Sie den Benutzernamen und das Kennwort eingeben.
3. Wenn Sie zweistufige Überprüfung eingerichtet haben, geben Sie den Einmal-Sicherheitscode ein, den Sie entweder per SMS erhalten haben oder der in Ihrer Authenticator-App erzeugt wurde (anhängig von der Methode der zweistufigen Überprüfung, die Sie eingerichtet haben).

   Auf der Seite des Portals wird das Unternehmen, in dem Sie über Administratorrechte verfügen, und eine Liste der Arbeitsbereiche angezeigt.
4. Klicken Sie im Abschnitt **Zum Löschen ausgewählt** im Block mit Informationen zum Arbeitsbereich auf den Link **Löschen abbrechen**.

Das Löschen des Arbeitsbereichs wird abgebrochen. Sie können wieder zum Arbeitsbereich wechseln und ihn weiterhin verwenden.

Den Zugriff auf das Unternehmen und seine Arbeitsbereiche verwalten

Dieser Abschnitt enthält Informationen über das Gewähren und Widerrufen des Zugriffs auf Ihr Unternehmen und seine Arbeitsbereiche.

Kaspersky Security Center Cloud Console bietet Ihnen zwei Zugriffsstufen:

- **Administrator**

  Ein Benutzer mit dieser Zugriffsstufe kann das Unternehmen und dessen Arbeitsbereiche in vollem Umfang verwalten.

- **Benutzer**

  Ein Benutzer mit dieser Zugriffsstufe kann die Liste der verfügbaren Arbeitsbereiche anzeigen und sich an diesen Arbeitsbereichen anmelden.

Zugriff auf Ihr Unternehmen und dessen Arbeitsbereiche gewähren

Sie können den Zugriff auf Ihr Unternehmen und seine Arbeitsbereiche gewähren, wenn Sie möchten, dass sich ein anderer Benutzer bei Ihrem Unternehmen anmelden kann und es entsprechend der gewählten Zugriffsstufe verwalten kann.

Bevor Sie einem Benutzer Zugriff gewähren können, muss der Benutzer ein Konto in der Kaspersky Security Center Cloud Console erstellen.

So gewähren Sie den Zugriff auf Ihr Unternehmen und seine Arbeitsbereiche:

1. Wechseln Sie in Ihrem Browser zur Kaspersky Security Center Cloud Console.
2. Melden Sie sich mit Ihrem Konto bei Kaspersky Security Center Cloud Console an, indem Sie den Benutzernamen und das Kennwort eingeben.
3. Wenn Sie zweistufige Überprüfung eingerichtet haben, geben Sie den Einmal-Sicherheitscode ein, den Sie entweder per SMS erhalten haben oder der in Ihrer Authenticator-App erzeugt wurde (anhängig von der Methode der zweistufigen Überprüfung, die Sie eingerichtet haben).

   Auf der Seite des Portals wird das Unternehmen, in dem Sie über Administratorrechte verfügen, und eine Liste der Arbeitsbereiche angezeigt.
4. Klicken Sie auf den Link **Zugriffskontrolle anzeigen**.

   Die Liste mit Konten, die Zugriff auf das Unternehmen haben, wird erweitert.
5. Klicken Sie auf den Link **Zugriff gewähren**.
6. Geben Sie im Feld **E-Mail-Adresse** die E-Mail-Adresse des Kontos an, dem Sie Zugriff gewähren möchten.
7. Wählen Sie in der Liste **Zugriffsstufe** die Zugriffsstufe aus, die Sie dem eingegebenen Konto zuweisen möchten:

   - **Administrator**

Ein Benutzer mit dieser Zugriffsstufe kann das Unternehmen und dessen Arbeitsbereiche in vollem Umfang verwalten.

- **Benutzer**

  Ein Benutzer mit dieser Zugriffsstufe kann die Liste der verfügbaren Arbeitsbereiche anzeigen und sich an diesen Arbeitsbereichen anmelden.

Sie können einem Konto nicht mehrere Zugriffsstufen innerhalb eines Unternehmens gewähren.

8. Klicken Sie auf **Gewähren**.

Dem angegebenen Konto wird Zugriff auf Ihr Unternehmen und seine Arbeitsbereiche gewährt. Der Benutzer kann sich an dem Unternehmen anmelden und es entsprechend der gewählten Zugriffsstufe verwalten.

Wenn Sie dem Konto die Zugriffsstufe **Benutzer** gewährt haben, müssen Sie dem hinzugefügten Benutzer eine Rolle zuweisen. Andernfalls kann sich der Benutzer nicht an dem Arbeitsbereich anmelden.

Den Zugriff auf Ihr Unternehmen und seine Arbeitsbereiche widerrufen

Sie können den Zugriff auf Ihr Unternehmen und seine Arbeitsbereiche widerrufen, wenn Sie nicht mehr möchten, dass sich ein Benutzer bei Ihrem Unternehmen anmelden und es verwalten kann (z. B. nachdem der Benutzer das Unternehmen verlässt).

Ihren eigenen Zugriff auf das Unternehmen können Sie nicht widerrufen.

So widerrufen Sie den Zugriff auf Ihr Unternehmen und seine Arbeitsbereiche:

1. Wechseln Sie in Ihrem Browser zur Kaspersky Security Center Cloud Console.
2. Melden Sie sich mit Ihrem Konto bei Kaspersky Security Center Cloud Console an, indem Sie den Benutzernamen und das Kennwort eingeben.
3. Wenn Sie zweistufige Überprüfung eingerichtet haben, geben Sie den Einmal-Sicherheitscode ein, den Sie entweder per SMS erhalten haben oder der in Ihrer Authenticator-App erzeugt wurde (anhängig von der Methode der zweistufigen Überprüfung, die Sie eingerichtet haben).

   Auf der Seite des Portals wird das Unternehmen, in dem Sie über Administratorrechte verfügen, und eine Liste der Arbeitsbereiche angezeigt.
4. Klicken Sie auf den Link **Zugriffskontrolle anzeigen**.

   Die Liste mit Konten, die Zugriff auf das Unternehmen haben, wird erweitert.
5. Klicken Sie neben dem Konto, dessen Zugriff Sie widerrufen möchten, auf das Symbol **Widerrufen** (🗑).
6. Klicken Sie im sich öffnenden Fenster **Zugriff auf das Unternehmen widerrufen** auf **OK**, um den Vorgang zu bestätigen.

Für das ausgewählt Konto wird der Zugriff auf Ihr Unternehmen und dessen Arbeitsbereiche widerrufen. Der Benutzer kann sich nicht mehr an dem Unternehmen anmelden und es verwalten.

Kennwort zurücksetzen

Wenn Sie das Kennwort für Ihr Konto in Kaspersky Security Center Cloud Console vergessen haben, können Sie den Zugriff auf Ihr Konto wiederherstellen, indem Sie Ihr Kennwort zurücksetzen.

Um das Kontokennwort zurückzusetzen, gehen Sie wie folgt vor:

1. Wechseln Sie in Ihrem Browser zur Kaspersky Security Center Cloud Console.
2. Klicken Sie auf die Schaltfläche **Anmelden** und klicken Sie dann auf den Link **Kennwort vergessen?**.
3. Geben Sie die E-Mail-Adresse ein, die Sie beim Erstellen des Kontos angegeben haben.
4. Klicken Sie auf **Kennwort zurücksetzen**.

   Eine E-Mail-Nachricht mit einem Link zum Zurücksetzen des Kennworts wird an die angegebene E-Mail-Adresse gesendet.
5. Klicken Sie auf den Link in der E-Mail-Nachricht.
6. Geben Sie im folgenden Fenster ein neues Kennwort ein und bestätigen Sie es.
7. Wenn Sie eine Geheimfrage festgelegt haben, beantworten Sie die Frage.

   Wenn Sie zweistufige Überprüfung eingerichtet haben, geben Sie den Einmal-Sicherheitscode ein, den Sie entweder per SMS erhalten haben oder der in Ihrer Authenticator-App erzeugt wurde (anhängig von der Methode der zweistufigen Überprüfung, die Sie eingerichtet haben).
8. Klicken Sie auf **Fortsetzen**.

   Das neue Kennwort für die Anmeldung bei Kaspersky Security Center Cloud Console wird gespeichert.

Wenn Sie keine E-Mail-Nachricht bekommen haben, prüfen Sie die angegebene E-Mail-Adresse und den Spam-Ordner und versuchen Sie es dann erneut. Wenn Sie auch nach dem erneuten Versuch keine Nachricht erhalten haben, ist die angegebene E-Mail-Adresse möglicherweise nicht auf der Website registriert. Bitte wenden Sie sich an den Technischen Support von Kaspersky.

Kontoeinstellungen in Kaspersky Security Center Cloud Console ändern

Dieser Abschnitt enthält Anweisungen zur Änderung und zum Löschen des Kontos in Kaspersky Security Center Cloud Console.

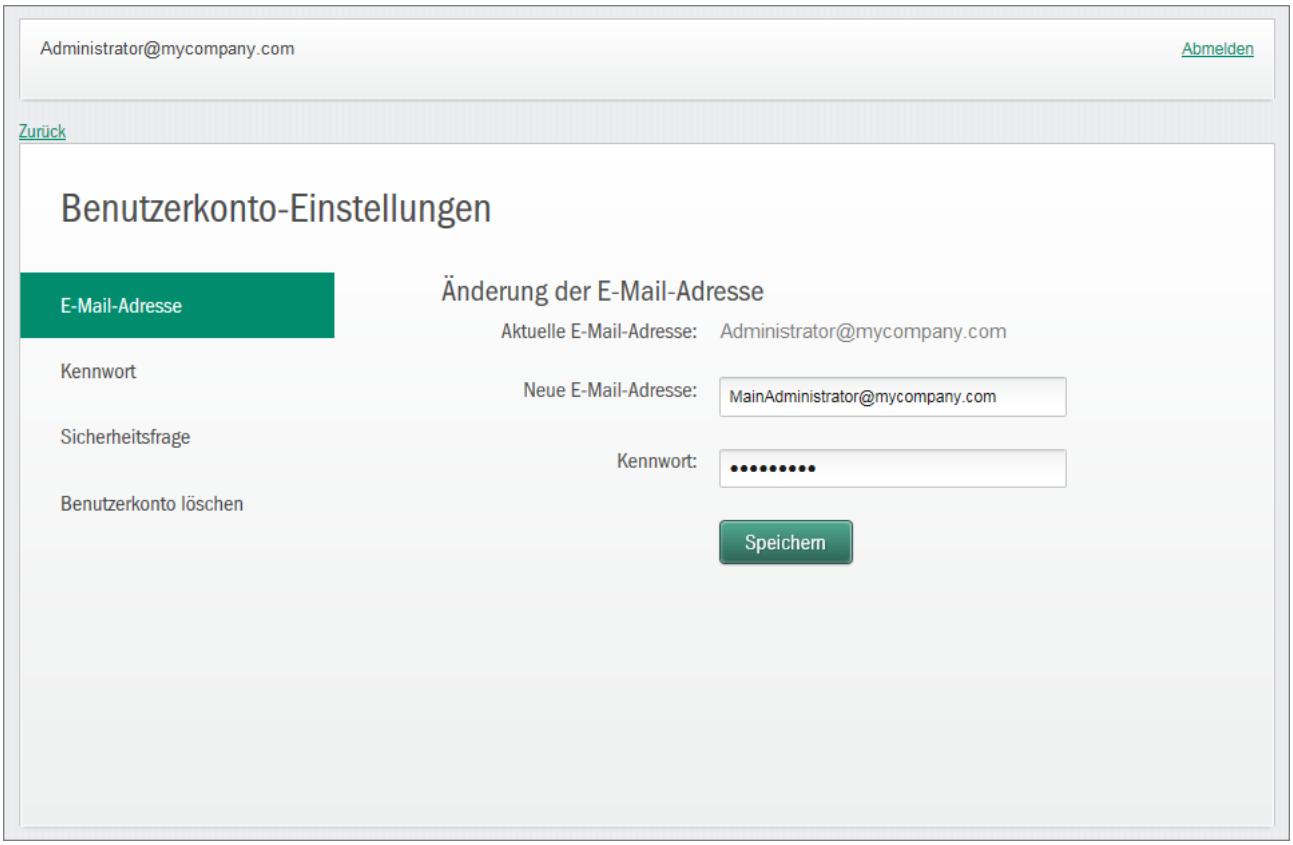
E-Mail-Adresse ändern

Um in den Kontoeinstellungen von Kaspersky Security Center Cloud Console Ihre E-Mail-Adresse zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie in der Kaspersky Security Center Cloud Console auf den Link mit dem Namen Ihres Kontos und wählen Sie die Option **Benutzerkonto verwalten** aus.

Das Fenster **Benutzerkonto-Einstellungen** wird geöffnet.

2. Wählen Sie den Abschnitt **E-Mail-Adresse** (s. Abb. unten).



E-Mail-Adresse in den Kontoeinstellungen von Kaspersky Security Center Cloud Console ändern

Im Abschnitt **E-Mail-Adresse** werden Ihre aktuelle E-Mail-Adresse, ein Eingabefeld für die neue Adresse, ein Eingabefeld für das Kennwort sowie die Schaltfläche **Speichern** angezeigt.

3. Geben Sie im Eingabefeld **Neue E-Mail-Adresse** Ihre neue E-Mail-Adresse ein.

   Bitte geben Sie die Adresse sorgfältig ein. Wenn Sie eine falsche Adresse eingeben, können Sie nicht auf Ihr Konto zugreifen und mit Kaspersky Security Center Cloud Console arbeiten.

4. Geben Sie im Eingabefeld **Kennwort** Ihr aktuelles Kennwort ein.

5. Klicken Sie auf **Speichern**.

6. Kehren Sie mithilfe des Links **Zurück** zu Kaspersky Security Center Cloud Console zurück oder beenden Sie die Arbeit mit dem Portal über den Link **Abmelden**.

Daraufhin wird Ihre E-Mail-Adresse in den Einstellungen des Benutzerkontos für Kaspersky Security Center Cloud Console und in den Einstellungen des Benutzerkontos für My Kaspersky geändert. An Ihre neue E-Mail-Adresse wird eine Nachricht mit einer Benachrichtigung über die Änderung der Adresse für den Zugriff auf das Konto gesendet. Von nun an müssen Sie die neue E-Mail-Adresse angeben, wenn Sie sich in Kaspersky Security Center Cloud Console anmelden.

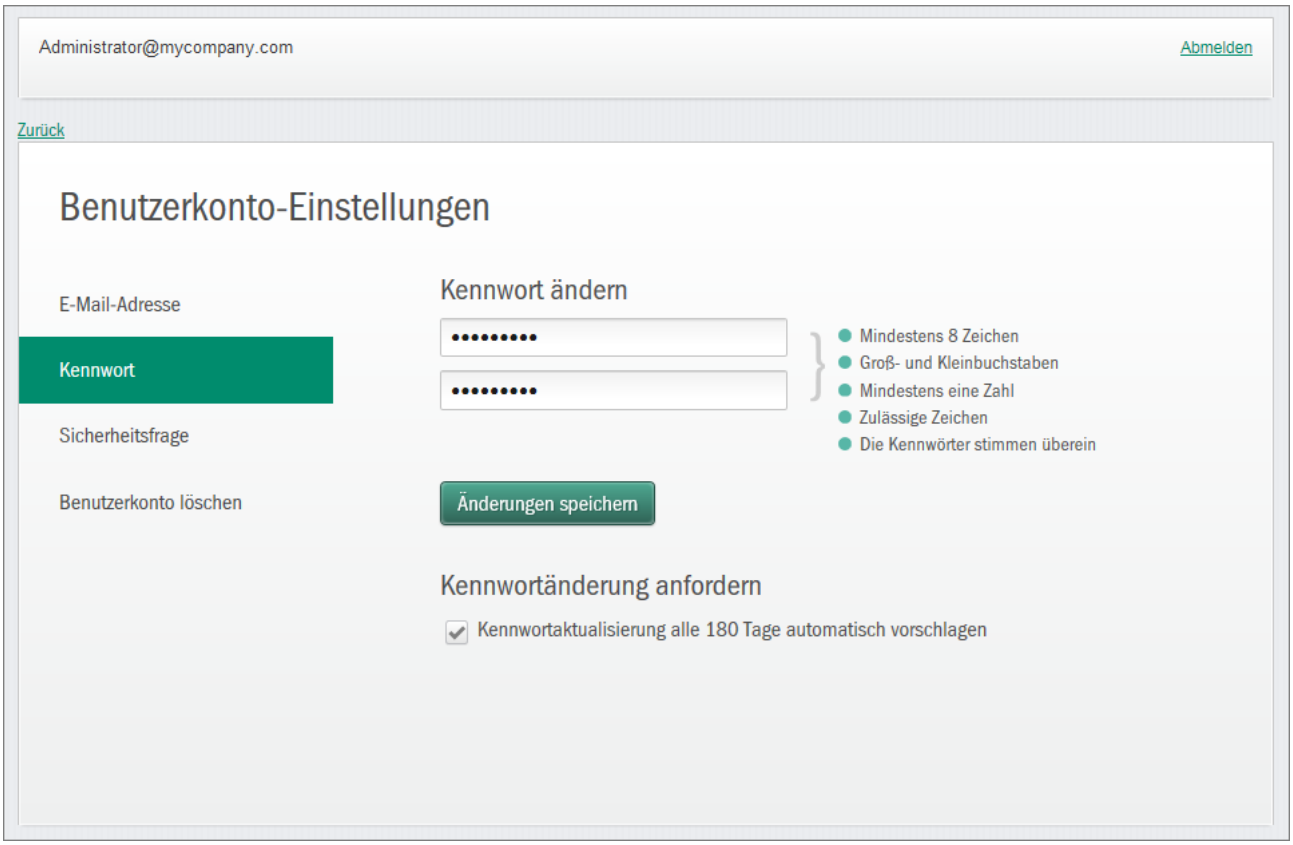
Kennwort ändern

Um in den Kontoeinstellungen von Kaspersky Security Center Cloud Console Ihr Kennwort zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie in der Kaspersky Security Center Cloud Console auf den Link mit dem Namen Ihres Kontos und wählen Sie die Option **Benutzerkonto verwalten** aus.

   Das Fenster **Benutzerkonto-Einstellungen** wird geöffnet.

2. Wählen Sie den Abschnitt **Kennwort** aus (s. Abb. unten).



Kennwort des Kontos in Kaspersky Security Center Cloud Console ändern

   In diesem Abschnitt werden Felder zur Eingabe des neuen Kennworts und dessen Bestätigung sowie die Schaltfläche **Änderungen speichern** angezeigt.

3. Geben Sie das neue Kennwort und dessen Bestätigung in die Eingabefelder ein.

   Rechts neben dem Eingabefeld für das Kennwort werden die Kennwortanforderungen angezeigt. Solange die Anforderungen nicht erfüllt sind, kann das Kennwort nicht gespeichert werden.

4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Kennwortaktualisierung alle 180 Tage automatisch fordern**.

   Dieses Kontrollkästchen ist standardmäßig ausgewählt.

5. Klicken Sie auf **Änderungen speichern**.

6. Kehren Sie mithilfe des Links **Zurück** zu Kaspersky Security Center Cloud Console zurück oder beenden Sie die Arbeit mit dem Portal über den Link **Abmelden**.

Ihr Kennwort ist jetzt geändert. Von nun an müssen Sie bei der Anmeldung an der Kaspersky Security Center Cloud Console und an My Kaspersky das neue Kennwort angeben.

Die zweistufige Überprüfung verwenden

In diesem Abschnitt wird die zweistufige Überprüfung beschrieben, mit deren Hilfe Sie die Sicherheit Ihres Kontos in der Kaspersky Security Center Cloud Console erhöhen können.

Über die zweistufige Überprüfung

Die zweistufige Überprüfung kann Ihnen dabei helfen, die Sicherheit Ihres Benutzerkontos in der Kaspersky Security Center Cloud Console zu erhöhen. Wenn diese Funktion aktiviert ist, müssen Sie jedes Mal, wenn Sie sich mit E-Mail-Adresse und Kennwort an der Kaspersky Security Center Cloud Console anmelden, einen zusätzlichen Einmal-Sicherheitscode eingeben. Mit einer zweistufigen Überprüfung können sich Kriminelle nicht bei Ihrem Konto anmelden, wenn Sie Ihr Kennwort gestohlen oder erraten haben, da sie darüber hinaus auch noch Zugriff auf Ihr Mobiltelefon haben müssen. Wenn die zweistufige Überprüfung aktiviert ist, müssen Sie außerdem einen zusätzlichen Einmal-Sicherheitscode eingeben, wenn Sie Ihr Kennwort verloren haben.

Nachdem Sie die zweistufige Überprüfung eingerichtet haben, sind Sie dafür verantwortlich, Ihr Mobiltelefon physikalisch sicher zu halten und den Zugriff auf Ihre Telefonnummer zu verwalten.

Sie erhalten einen Einmal-Sicherheitscode auf eine der folgenden Arten:

- Der Sicherheitscode wird per SMS an Ihr Mobiltelefon gesendet.

  Wenn Sie in diesem Szenario den Zugriff auf Ihr Mobiltelefon verlieren, können Sie sich so lange nicht mit Ihrem Konto an der Kaspersky Security Center Cloud Console anmelden, bis Sie wieder Zugriff auf Ihre Telefon haben.

- Der Sicherheitscode wird in einer Authenticator-App erstellt, die auf Ihrem Mobiltelefon installiert ist.

  Es wird dringend empfohlen, dass Sie die zweistufige Überprüfung unter Verwendung einer Authenticator-App einrichten. In diesem Fall können Sie sich selbst dann an Ihrem Benutzerkonto anmelden, wenn Ihr Mobiltelefon nicht mit dem Internet oder einem Mobilfunknetz verbunden ist.

  Auf Kompatibilität mit Kaspersky Security Center Cloud Console wurden nur Google Authenticator und Microsoft Authenticator getestet. Diese Apps konnten zu diesem Zeitpunkt kostenlos genutzt werden. Möglicherweise ist die Benutzeroberfläche dieser Apps in Ihrer bevorzugten Sprache nicht verfügbar. Bitte überprüfen Sie auch die Übereinstimmung dieser Apps mit der DSGVO und der Datenschutzrichtlinie, bevor Sie diese nutzen. Kaspersky wird in keiner Weise von den Eigentümern dieser Apps gesponsert oder unterstützt oder steht mit diesen in einer Verbindung.

  > Der Microsoft Authenticator kann nur auf mobilen Geräten installiert werden.

  Es wird außerdem empfohlen, dass Sie eine Authenticator-App auf einem weiteren Gerät neben Ihren Mobiltelefon installieren. Dadurch können Sie sich weiterhin an Ihrem Benutzerkonto anmelden, falls Ihr Mobiltelefon verloren geht oder gestohlen wird.

  Wenn Sie in diesem Szenario den Zugriff auf Ihr Mobiltelefon verlieren und auf einem weiteren Gerät keine Authenticator-App installiert ist, können Sie sich so lange nicht mit Ihrem Konto an der Kaspersky Security Center Cloud Console anmelden, bis Sie wieder Zugriff auf Ihre Telefon haben. Verwenden Sie anschließend den Sicherheitscode, der per SMS gesendet wird.

> Wenn Sie zuvor eine Geheimfrage festgelegt haben, um Ihr Kennwort bei Verlust wiederherzustellen, wird die Sicherheitsfrage dauerhaft deaktiviert, wenn Sie eine zweistufige Überprüfung einrichten.

Szenario: Einrichten der zweistufigen Überprüfung

Die zweistufige Überprüfung kann Ihnen dabei helfen, die Sicherheit Ihres Benutzerkontos in der Kaspersky Security Center Cloud Console zu erhöhen. Nachdem Sie das Szenario in diesem Abschnitt abgeschlossen haben, ist die zweistufige Überprüfung eingerichtet.

Das Szenario verläuft in den folgenden Schritten:

1. **Angeben Ihrer Telefonnummer**

   In diesem Schritt wird die zweistufige Überprüfung per SMS eingerichtet.

2. **Installieren und Konfigurieren einer Authenticator-App**

   Installation und Konfiguration einer Authenticator-App.

   Es wird dringend empfohlen, dass Sie die zweistufige Überprüfung unter Verwendung einer Authenticator-App einrichten. In diesem Fall können Sie sich selbst dann an Ihrem Benutzerkonto anmelden, wenn Ihr Mobiltelefon nicht mit dem Internet oder einem Mobilfunknetz verbunden ist.

   Es wird außerdem empfohlen, dass Sie eine Authenticator-App auf einem weiteren Gerät neben Ihren Mobiltelefon installieren. Dadurch können Sie sich weiterhin an Ihrem Benutzerkonto anmelden, falls Ihr Mobiltelefon verloren geht oder gestohlen wird.

3. **Ändern Ihrer Telefonnummer**

   Bei Bedarf können Sie die Telefonnummer ändern, die Sie für die zweistufige Überprüfung verwenden.

Zweistufige Überprüfung mittels SMS einrichten

Um die zweistufige Überprüfung mittels SMS einrichten, gehen Sie wie folgt vor:

1. Klicken Sie in der Kaspersky Security Center Cloud Console auf den Link mit dem Namen Ihres Kontos und wählen Sie die Option **Benutzerkonto verwalten** aus.

   Das Fenster **Benutzerkonto-Einstellungen** wird geöffnet.

2. Wählen Sie den Abschnitt **Zweistufige Überprüfung** aus.

3. Klicken Sie auf die Schaltfläche **Einrichten**.

4. Geben Sie unter **Aktuelles Kennwort eingeben** das Kennwort für Ihr Konto in der Kaspersky Security Center Cloud Console ein und klicken Sie anschließend auf die Schaltfläche **Weiter**.

5. Geben Sie unter **Mobiltelefonnummer angeben** die Mobiltelefonnummer an, die Sie für zweistufige Überprüfung verwenden möchten, und klicken Sie anschließend auf die Schaltfläche **Weiter**.

   > Sie können dieselbe Telefonnummer für bis zu fünf Konten verwenden.

   An die angegebene Telefonnummer wird ein 6-stelliger Sicherheitscode gesendet.

6. Geben Sie unter **Bestätigen Sie Ihre Telefonnummer** den erhaltenen Sicherheitscode ein.

Die zweistufige Überprüfung wird eingerichtet. Jetzt müssen Sie jedes Mal, wenn Sie sich mit E-Mail-Adresse und Kennwort anmelden, oder wenn Sie ihr Kennwort verloren haben, einen Einmal-Sicherheitscode eingeben, den Sie per SMS an die angegebene Telefonnummer erhalten.

Sie können jetzt eine Authenticator-App installieren und konfigurieren, Ihre Telefonnummer ändern oder die zweistufige Überprüfung deaktivieren.

Zweistufige Überprüfung mittels einer Authenticator-App einrichten

Authentifikator-Apps können in Kaspersky Security Center Cloud Console nicht als eigenständige Authentifikationsmethode verwendet werden. Sie müssen zuerst die zweistufige Überprüfung mittels SMS einrichten. Wenn Sie die zweistufige Überprüfung über Ihre Mobiltelefonnummer deaktivieren, wird die Authentifikation über eine Authenticator-App automatisch abgeschaltet. Nachdem Sie eine Authentifikation über SMS und über eine App eingerichtet haben, können Sie sowohl auf der Anmeldeseite als auch bei verlorenem Kennwort eine Methode zur Authentifikation auswählen.

Um die zweistufige Überprüfung mittels einer Authenticator-App einzurichten, gehen Sie wie folgt vor:

1. Zweistufige Überprüfung mittels SMS einrichten.

2. Laden Sie die gewünschte Authenticator-App herunter und installieren und starten Sie diese.

   Auf Kompatibilität mit Kaspersky Security Center Cloud Console wurden nur Google Authenticator und Microsoft Authenticator getestet. Diese Apps konnten zu diesem Zeitpunkt kostenlos genutzt werden. Möglicherweise ist die Benutzeroberfläche dieser Apps in Ihrer bevorzugten Sprache nicht verfügbar. Bitte überprüfen Sie auch die Übereinstimmung dieser Apps mit der DSGVO und der Datenschutzrichtlinie, bevor Sie diese nutzen. Kaspersky wird in keiner Weise von den Eigentümern dieser Apps gesponsert oder unterstützt oder steht mit diesen in einer Verbindung.

   > Der Microsoft Authenticator kann nur auf mobilen Geräten installiert werden.

   Sie können auf eigenes Risiko natürlich auch andere Apps verwenden. Die App, die Sie verwenden, muss 6-stellige Sicherheitscodes unterstützen.

   Es wird außerdem empfohlen, dass Sie eine Authenticator-App auf einem weiteren Gerät neben Ihren Mobiltelefon installieren. Dadurch können Sie sich weiterhin an Ihrem Benutzerkonto anmelden, falls Ihr Mobiltelefon verloren geht oder gestohlen wird.

3. Klicken Sie in der Kaspersky Security Center Cloud Console auf den Link mit dem Namen Ihres Kontos und wählen Sie die Option **Benutzerkonto verwalten** aus.

   Das Fenster **Benutzerkonto-Einstellungen** wird geöffnet.

4. Wählen Sie den Abschnitt **Zweistufige Überprüfung** aus.

5. Klicken Sie auf die Schaltfläche **Geheimen Schlüssel erzeugen**.

6. Geben Sie unter **Aktuelles Kennwort eingeben** das Kennwort für Ihr Konto in der Kaspersky Security Center Cloud Console ein und klicken Sie anschließend auf die Schaltfläche **Weiter**.

   Auf der Portalseite werden ein 16-stelliger geheimer Schlüssel und ein QR-Code angezeigt.

7. Erstellen Sie in der Authenticator-App auf jedem Gerät ein Konto und geben Sie den angezeigten geheimen Schlüssel ein. Alternativ dazu können Sie auch den QR-Code mit Ihrem Mobiltelefon scannen. In diesem Fall wird das Konto automatisch erstellt. Weitere Informationen erhalten Sie in der Dokumentation der jeweiligen App.

   In Ihren Authenticator-App wird ein 6-stelliger Sicherheitscode erzeugt.

8. Überprüfen Sie, ob die in Ihren Apps erzeugten Sicherheitscodes auf jedem Gerät dieselben sind.

9. Geben Sie in Kaspersky Security Center Cloud Console den erzeugten Sicherheitscode ein.

Die zweistufige Überprüfung mittels einer Authenticator-App ist eingerichtet. Jetzt müssen Sie jedes Mal, wenn Sie sich mit E-Mail-Adresse und Kennwort anmelden, oder wenn Sie ihr Kennwort verloren haben, einen Einmal-Sicherheitscode eingeben, der in Ihrer Authenticator-App erzeugt wird.

Sie können jetzt die Verwendung einer Authenticator-App deaktivieren oder die zweistufige Überprüfung vollständig deaktivieren.

Telefonnummer ändern

Um die Mobiltelefonnummer zu ändern, die für die zweistufige Überprüfung mittels SMS verwendet wird, gehen Sie wie folgt vor:

1. Klicken Sie in der Kaspersky Security Center Cloud Console auf den Link mit dem Namen Ihres Kontos und wählen Sie die Option **Benutzerkonto verwalten** aus.

   Das Fenster **Benutzerkonto-Einstellungen** wird geöffnet.

2. Wählen Sie den Abschnitt **Zweistufige Überprüfung** aus.

3. Klicken Sie unter **Telefonnummer** auf den Link **Telefonnummer ändern**.

4. Geben Sie unter **Mobiltelefonnummer angeben** die neue Mobiltelefonnummer an, die Sie für die zweistufige Überprüfung verwenden möchten, und klicken Sie anschließend auf die Schaltfläche **Weiter**.

5. Geben Sie unter **Aktuelles Kennwort eingeben** das Kennwort für Ihr Konto in der Kaspersky Security Center Cloud Console ein und klicken Sie anschließend auf die Schaltfläche **Weiter**.

   An die angegebene Telefonnummer wird ein 6-stelliger Sicherheitscode gesendet.

6. Geben Sie unter **Bestätigen Sie Ihre Telefonnummer** den erhaltenen Sicherheitscode ein.

Ihre Telefonnummer wird geändert. Einmal-Sicherheitscodes werden jetzt an die neue Telefonnummer gesendet.

Zweistufige Überprüfung deaktivieren

Wenn Sie die zweistufige Überprüfung nicht mehr verwenden möchten, können Sie diese wie in diesem Abschnitt beschrieben deaktivieren.

Durch die Deaktivierung der zweistufigen Überprüfung wird die Sicherheit Ihres Kontos verringert. Es wird dringend empfohlen, weiterhin eine zweistufige Überprüfung zu verwenden.

Wenn Sie die zweistufige Überprüfung mittels SMS einrichten, können Sie die zweistufige Überprüfung deaktivieren. Wenn Sie die zweistufige Überprüfung mittels einer Authenticator-App einrichten, können Sie die Verwendung der App deaktivieren oder die zweistufige Überprüfung vollständig deaktivieren.

Um die Verwendung einer Authenticator-App zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie in der Kaspersky Security Center Cloud Console auf den Link mit dem Namen Ihres Kontos und wählen Sie die Option **Benutzerkonto verwalten** aus.

   Das Fenster **Benutzerkonto-Einstellungen** wird geöffnet.

2. Wählen Sie den Abschnitt **Zweistufige Überprüfung** aus.

3. Klicken Sie unter **Authenticator-App** auf den Link **Verwendung der Authentifizierungs-App deaktivieren**.

4. Geben Sie unter **Aktuelles Kennwort eingeben** das Kennwort für Ihr Konto in der Kaspersky Security Center Cloud Console ein und klicken Sie anschließend auf die Schaltfläche **Weiter**.

Die Verwendung der Authenticator-App wird deaktiviert. Die Einstellungen für die zweistufige Überprüfung mittels einer Authenticator-App werden gelöscht. Sie können die Konten in Ihren Authenticator-App jetzt löschen.

Sie können später die zweistufige Überprüfung mittels einer Authenticator-App erneut einrichten.

Um die zweistufige Überprüfung vollständig zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie in der Kaspersky Security Center Cloud Console auf den Link mit dem Namen Ihres Kontos und wählen Sie die Option **Benutzerkonto verwalten** aus.

   Das Fenster **Benutzerkonto-Einstellungen** wird geöffnet.

2. Wählen Sie den Abschnitt **Zweistufige Überprüfung** aus.

3. Klicken Sie unter **Telefonnummer** auf den Link **Zweistufige Überprüfung deaktivieren**.

4. Geben Sie unter **Aktuelles Kennwort eingeben** das Kennwort für Ihr Konto in der Kaspersky Security Center Cloud Console ein und klicken Sie anschließend auf die Schaltfläche **Weiter**.

Die zweistufige Überprüfung wird deaktiviert. Wenn Sie die zweistufige Überprüfung mittels einer Authenticator-App verwendet haben, werden die Einstellungen für die zweistufige Überprüfung gelöscht. Sie können die Konten in Ihren Authenticator-App jetzt löschen.

Sie können später die zweistufige Überprüfung erneut einrichten.

Löschen eines Kontos in Kaspersky Security Center Cloud Console

Wenn Sie die Benutzung von Kaspersky Security Center Cloud Console einstellen wollen, können Sie Ihr Konto löschen.

Beim Löschen des Kontos gehen sämtliche mit diesem Konto verknüpften Informationen verloren.

Nachdem Sie Ihr Konto gelöscht haben, können Sie nicht mehr auf Ihre Arbeitsbereiche in Kaspersky Endpoint Security Cloud, Kaspersky Security für Microsoft Office 365 und Kaspersky Security Center Cloud Console zugreifen. Wenn Sie der einzige Administrator in einem Arbeitsbereich waren, wird der Arbeitsbereich ordnungsgemäß gelöscht. Außerdem verlieren Sie den Zugriff auf Ihr Konto in My Kaspersky.

So löschen Sie ein Konto in Kaspersky Security Center Cloud Console:

1. Klicken Sie in der Kaspersky Security Center Cloud Console auf den Link mit dem Namen Ihres Kontos und wählen Sie die Option **Benutzerkonto verwalten** aus.

   Das Fenster **Benutzerkonto-Einstellungen** wird geöffnet.

2. Wählen Sie den Abschnitt **Benutzerkonto löschen** aus.

Im Abschnitt **Benutzerkonto löschen** werden Informationen über die Auswirkungen des Löschens eines Kontos angezeigt. Darunter befindet sich die Schaltfläche **Löschen**.

3. Lesen Sie die Informationen zum Löschen des Kontos und klicken Sie auf die Schaltfläche **Löschen**.

   Das Fenster **Geben Sie das Kennwort für Ihr Benutzerkonto ein** wird angezeigt.

4. Geben Sie im Feld zur Kennworteingabe Ihr Kennwort ein und klicken Sie anschließend auf die Schaltfläche **Weiter**.

Ihr Konto wird gelöscht.

Auswahl der Rechenzentren für die Speicherung der Informationen in Kaspersky Security Center Cloud Console

Zu Erstellung eines Arbeitsbereichs für Kaspersky Security Center Cloud Console werden Server aus einem Netzwerk globaler Rechenzentren auf Basis der Cloud-Plattform Microsoft Azure verwendet. Die Auswahl des Rechenzentrums als Speicherort des Arbeitsbereichs ist abhängig vom Land, das Sie bei der Registrierung des Arbeitsbereichs in Kaspersky Security Center Cloud Console angegeben haben (s. Tabelle unten). Die Pakete der Sicherheitsanwendungen werden auf den selben Servern wie die Arbeitsbereiche gespeichert.

Zugehörigkeit des Landes des Unternehmens zur Microsoft Azure-Region

Land, in dem sich das Unternehmen befindet	Region des Microsoft-Rechenzentrums
Argentinien	Brasilien, Süden
Bolivien	Brasilien, Süden
Brasilien	Brasilien, Süden
Chile	Brasilien, Süden
Kolumbien	Brasilien, Süden
Ecuador	Brasilien, Süden
Guyana	Brasilien, Süden
Peru	Brasilien, Süden
Paraguay	Brasilien, Süden
Suriname	Brasilien, Süden
Uruguay	Brasilien, Süden
Venezuela	Brasilien, Süden
Antigua und Barbuda	USA, Osten
Anguilla	USA, Osten
Aruba	USA, Osten
Barbados	USA, Osten
Sankt Bartholomäus	USA, Osten
Bonaire, Sint Eustatius und Saba	USA, Osten
Belize	USA, Osten
Costa Rica	USA, Osten

Kuba	USA, Osten
Curaçao	USA, Osten
Dominica	USA, Osten
Dominikanische Republik	USA, Osten
Grenada	USA, Osten
Guadeloupe	USA, Osten
Guatemala	USA, Osten
Honduras	USA, Osten
Haiti	USA, Osten
Jamaika	USA, Osten
St. Kitts und Nevis	USA, Osten
Cayman Islands	USA, Osten
St. Lucia	USA, Osten
Saint-Martin	USA, Osten
Martinique	USA, Osten
Montserrat	USA, Osten
Nicaragua	USA, Osten
Panama	USA, Osten
Puerto Rico	USA, Osten
Sint Maarten	USA, Osten
Trinidad und Tobago	USA, Osten
St. Vincent und die Grenadinen	USA, Osten
Jungferninseln (Großbritannien)	USA, Osten
Jungferninseln (USA)	USA, Osten
Japan	USA, Osten
Kanada (Neubraunschweig)	USA, Osten
Kanada (Neufundland und Labrador)	USA, Osten
Kanada (Neuschottland)	USA, Osten
Kanada (Ontario)	USA, Osten
Kanada (Prince-Edward-Insel)	USA, Osten
Kanada (Quebec)	USA, Osten
USA (Alabama)	USA, Osten
USA (Arkansas)	USA, Osten
USA (Connecticut)	USA, Osten
USA (District of Columbia)	USA, Osten
USA (Delaware)	USA, Osten

USA (Florida)	USA, Osten
USA (Georgia)	USA, Osten
USA (Iowa)	USA, Osten
USA (Illinois)	USA, Osten
USA (Indiana)	USA, Osten
USA (Kentucky)	USA, Osten
USA (Louisiana)	USA, Osten
USA (Massachusetts)	USA, Osten
USA (Maryland)	USA, Osten
USA (Maine)	USA, Osten
USA (Michigan)	USA, Osten
USA (Minnesota)	USA, Osten
USA (Missouri)	USA, Osten
USA (Mississippi)	USA, Osten
USA (North Carolina)	USA, Osten
USA (New Hampshire)	USA, Osten
USA (New Jersey)	USA, Osten
USA (New York)	USA, Osten
USA (Ohio)	USA, Osten
USA (Pennsylvania)	USA, Osten
USA (Rhode Island)	USA, Osten
USA (South Carolina)	USA, Osten
USA (Tennessee)	USA, Osten
USA (Virginia)	USA, Osten
USA (Vermont)	USA, Osten
USA (Wisconsin)	USA, Osten
USA (West Virginia)	USA, Osten
Albanien	Europa, Norden (Irland)
Bosnien-Herzegowina	Europa, Norden (Irland)
Bulgarien	Europa, Norden (Irland)
Weißrussland	Europa, Norden (Irland)
Tschechien	Europa, Norden (Irland)
Dänemark	Europa, Norden (Irland)
Estland	Europa, Norden (Irland)
Finnland	Europa, Norden (Irland)
Großbritannien	Europa, Norden (Irland)

Grönland	Europa, Norden (Irland)
Griechenland	Europa, Norden (Irland)
Kroatien	Europa, Norden (Irland)
Ungarn	Europa, Norden (Irland)
Irland	Europa, Norden (Irland)
Island	Europa, Norden (Irland)
Kirgisistan	Europa, Norden (Irland)
Kasachstan	Europa, Norden (Irland)
Litauen	Europa, Norden (Irland)
Lettland	Europa, Norden (Irland)
Moldawien	Europa, Norden (Irland)
Montenegro	Europa, Norden (Irland)
Mazedonien	Europa, Norden (Irland)
Mongolei	Europa, Norden (Irland)
Norwegen	Europa, Norden (Irland)
Polen	Europa, Norden (Irland)
Rumänien	Europa, Norden (Irland)
Serbien	Europa, Norden (Irland)
Russland	Europa, Norden (Irland)
Schweden	Europa, Norden (Irland)
Slowenien	Europa, Norden (Irland)
Slowakei	Europa, Norden (Irland)
Tadschikistan	Europa, Norden (Irland)
Turkmenistan	Europa, Norden (Irland)
Usbekistan	Europa, Norden (Irland)
Kanada (Alberta)	USA, Westen
Kanada (Britisch-Kolumbien)	USA, Westen
Kanada (Manitoba)	USA, Westen
Kanada (Nordwest-Territorien)	USA, Westen
Kanada (Nunavut)	USA, Westen
Kanada (Yukon)	USA, Westen
Kanada (Saskatchewan)	USA, Westen
Mexiko	USA, Westen
USA (Alaska)	USA, Westen
USA (Arizona)	USA, Westen
USA (Kalifornien)	USA, Westen

USA (Colorado)	USA, Westen
USA (Hawaii)	USA, Westen
USA (Idaho)	USA, Westen
USA (Kansas)	USA, Westen
USA (Montana)	USA, Westen
USA (North Dakota)	USA, Westen
USA (Nebraska)	USA, Westen
USA (New Mexico)	USA, Westen
USA (Nevada)	USA, Westen
USA (Oklahoma)	USA, Westen
USA (Oregon)	USA, Westen
USA (South Dakota)	USA, Westen
USA (Texas)	USA, Westen
USA (Utah)	USA, Westen
USA (Washington)	USA, Westen
USA (Wyoming)	USA, Westen
USA (andere Verwaltungseinheiten)	USA, Osten
Andere Länder	Europa, Westen (Niederlande)

Zugriff auf öffentliche DNS-Server

Wenn der Zugriff auf die Kaspersky-Server über System-DNS nicht möglich ist, kann Kaspersky Security Center Cloud Console diese öffentlichen DNS-Server in der folgenden Reihenfolge verwenden:

1. Google Public DNS (8.8.8.8)
2. Cloudflare DNS (1.1.1.1)
3. Alibaba Cloud DNS (223.6.6.6)
4. Quad9 DNS (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

Anfragen an diese DNS-Server können Domänenadressen und die öffentliche IP-Adresse der Client-Geräte enthalten, da der Administrationsagent eine TCP/UDP-Verbindung zum DNS-Server herstellt. Wenn Kaspersky Security Center Cloud Console einen öffentlichen DNS-Server verwendet, unterliegt die Datenverarbeitung der Datenschutzrichtlinie des entsprechenden Dienstes.

Szenario: Erstellen einer Hierarchie von Administrationsservern, die durch Kaspersky Security Center Cloud Console verwaltet wird

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

Kaspersky Security Center Cloud Console 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 Security Center Cloud Console verwalten möchten, wurden installiert.
- Die verwalteten Programme wurden auf Versionen aktualisiert, die von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console alle Richtlinien und Aufgaben, bevor Sie die Hierarchie erstellen. Alternativ können Sie den Status jeder Richtlinie in Kaspersky Security Center Cloud Console in ihren Einstellungen auf **Inaktiv** ändern, und in den Einstellungen für jede Aufgabe in Kaspersky Security Center Cloud Console 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 Security Center Cloud Console**

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

   Öffnen Sie in Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 angegebenen 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 **Verbindungseinstellungen des sekundären Administrationsservers mit dem primären Administrationsserver festlegen** können Sie die Verwendung von Proxy-Servern konfigurieren, falls notwendig. Aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben Sie die folgenden Einstellungen an:

   - 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 **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:

   - HDS-Serveradresse (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 Security Center Cloud Console kopiert und gespeichert haben.

   - HDS-Serverports

     Geben Sie Nummer(n) des/der HDS-Serverports an, den/die Sie aus den Einstellungen des Administrationsservers in Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console gespeichert haben.

Wenn Sie bei der Verbindung des sekundären Administrationsservers in Kaspersky Security Center Cloud Console die Verwendung eines Proxyservers aktiviert haben, wählen Sie das Kontrollkästchen **Proxyserver verwenden** aus und geben Sie die gleichen Proxyeinstellungen wie in Kaspersky Security Center Cloud Console 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 (**Geräte→ Richtlinien und Profile**).
- Die vom primären Administrationsserver verteilten Gruppenaufgaben werden in dem sekundären Administrationsserver in der Liste der Aufgaben angezeigt (**Geräte → Aufgaben**).
- Richtlinien und Aufgaben, die auf dem primären Administrationsserver erstellt wurden, können in dem sekundären Administrationsserver nicht angepasst werden.
- In Kaspersky Security Center Cloud Console wird der sekundäre Administrationsserver innerhalb der Struktur der Administrationsgruppen in der Gruppe angezeigt, die Sie beim Hinzufügen dieses Administrationsservers festgelegt haben.

Migration nach Kaspersky Security Center Cloud Console

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 Security Center Cloud Console.

Methoden der Migration auf Kaspersky Security Center Cloud Console

Dieser Abschnitt enthält Informationen zu den zur Verfügung stehenden Methoden für die Migration von einem lokal ausgeführten Kaspersky Security Center auf Kaspersky Security Center Cloud Console.

Mit der Migrationsfunktion können Sie vernetzte Geräte aus Kaspersky Security Center unter die Verwaltung von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console auswählen:

- Migration ohne Hierarchie von Administrationsservern:
  - Macht den Wechsel der verwalteten Geräte und zugehörigen Objekten zu Kaspersky Security Center Cloud Console selbst dann möglich, wenn der lokal ausgeführte Administrationsserver kein sekundärer Server in Bezug auf Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console durch ausschließliche Verwendung der Benutzeroberfläche von Kaspersky Security Center Cloud Console möglich. Es wird daher kein physisches Übertragen von Daten benötigt.
  - Dies setzt voraus, dass der lokal ausgeführte Administrationsserver als sekundärer Server von Kaspersky Security Center Cloud Console fungiert. Sie können eine derartige Hierarchie vor dem Beginn der Migration erzeugen.

Für die vollständige Festplattenverschlüsselung wird von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console. Sie können eine einzelne Administrationsgruppe in den Migrationsbereich aufnehmen, um dieselbe Administrationsgruppe in Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console und der lokal ausgeführten Kaspersky Security Center Web Console bestanden hat.

Erforderliche Vorrausetzungen

Führen Sie vor dem Start Folgendes durch:

- Aktualisierung des lokal ausgeführten Administrationsservers auf folgende Version:
  - Für Windows-Geräte – Version 12 oder höher
  - Für Linux-Geräte – Version 12 Patch A oder höher
- Installation von Kaspersky Security Center Web Console in Version 12.1 oder höher.
- Aktualisierung des Administrationsagenten auf den verwalteten Geräten auf 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 eines Programms* eine Remote-Deinstallation des Administrationsagenten durch. Wählen Sie im Feld **Zu deinstallierendes Programm** 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 Security Center Cloud Console 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 für die Programmversionen, die von Kaspersky Security Center Cloud Console unterstützt werden.
- Um aktuelle Richtlinien zu verwenden, aktualisieren Sie die Web-Plug-ins, für die Programme, die Sie durch Kaspersky Security Center Cloud Console verwalten möchten.
- Deinstallieren Sie Kaspersky-Programme, die von Kaspersky Security Center Cloud Console nicht unterstützt werden, von den verwalteten Geräten und ersetzen Sie anschließend die deinstallierten Programme durch

unterstützte.

- Entschlüsseln Sie alle durch Kaspersky Endpoint Security für Windows auf verwalteten Windows-Geräten verschlüsselten Daten (auf Festplatten- oder Dateiebene) und deaktivieren Sie die Verschlüsselungsfunktion auf den verwalteten Geräten entweder lokal oder mittels Programmrichtlinie. 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 Security Center Cloud Console unterstützt maximal 25.000 verwaltete Geräte pro Administrationsserver.

Schritte der Migration

Die Migration auf Kaspersky Security Center Cloud Console 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 Security Center Cloud Console**

   Übertragen Sie die Informationen über Ihre verwalteten Geräte und Objekte an Kaspersky Security Center Cloud Console. Verwenden Sie zu diesem Zweck den Migrationsassistenten der Kaspersky Security Center Cloud Console, 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 Security Center Cloud Console verwaltet.
- Alle Objekteinstellungen, die vor der Migration wirksam waren, sind erhalten geblieben.

Migrationsassistent

Dieser Abschnitt enthält Informationen zu den Migrationsassistenten in Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Richtungspfeil (>) neben dem Gruppennamen **Verwaltete Geräte**, um die Hierarchie der Verwaltungsgruppen zu erweitern. Wählen Sie die Administrationsgruppe aus, die Sie exportieren möchten.
4. Wählen Sie die verwalteten Programme aus, deren Richtlinien und Aufgaben zusammen mit Gruppenobjekten an Kaspersky Security Center Cloud Console 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 Security Center Cloud Console unterstützt werden, klicken Sie auf den entsprechenden Link. Dieser öffnet in der Online-Hilfe einen Abschnitt mit einer Liste verwalteter Programme, die von Kaspersky Security Center Cloud Console unterstützt werden.

   Wenn Sie Anwendungen auswählen, die von der Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 globalen Aufgaben der verwalteten Programme 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 Security Center Cloud Console 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:

- Administrationsgruppenstruktur, 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 Programme

  Richtlinien des Administrationsservers und des Administrationsagenten werden nicht exportiert.

- Gruppenaufgaben der ausgewählten verwalteten Programme 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 Security Center Cloud Console 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 Security Center Cloud Console ausgeführt wird.

Wenn Sie Kaspersky Security Center Web Console und Kaspersky Security Center Cloud Console 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 Security Center Cloud Console

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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console zu importieren:

1. Wechseln Sie im Hauptmenü der Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console importiert wurden. Wechseln Sie dafür in den Abschnitt **Geräte** und prüfen Sie, ob in den Listen der Unterabschnitte **Richtlinien und Profile**, **Aufgaben**, und **Verwaltete 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 Security Center Cloud Console.

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 Softwareverteilung** → **Softwareverteilung 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console verwalten können. Wechseln Sie dazu nach **Geräte** → **Verwaltete 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 Security Center Cloud Console. Der Prozess umfasst eine Hierarchie: Die lokal ausgeführte Kaspersky Security Center Web Console fungiert als sekundärer Administrationsserver und Kaspersky Security Center Cloud Console fungiert als primärer Administrationsserver.

Jede Administrationsgruppe, die Sie an die Kaspersky Security Center Cloud Console 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 Security Center Cloud Console verwaltet.

Führen Sie vor dem Start Folgendes durch:

- Aktualisierung des lokal ausgeführten Administrationsservers auf folgende Version:
  - Für Windows-Geräte – Version 12 oder höher
  - Für Linux-Geräte – Version 12 Patch A oder höher
- Installation von Kaspersky Security Center Web Console in Version 12.1 oder höher.
- Aktualisierung des Administrationsagenten auf den verwalteten Geräten auf 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 eines Programms* eine Remote-Deinstallation des Administrationsagenten durch. Wählen Sie im Feld **Zu deinstallierendes Programm** 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 Security Center Cloud Console 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 für die Programmversionen, die von Kaspersky Security Center Cloud Console unterstützt werden.

- Um aktuelle Richtlinien zu verwenden, aktualisieren Sie die Web-Plug-ins, für die Programme, die Sie durch Kaspersky Security Center Cloud Console verwalten möchten.

- Deinstallieren Sie Kaspersky-Programme, die von Kaspersky Security Center Cloud Console nicht unterstützt werden, von den verwalteten Geräten und ersetzen Sie anschließend die deinstallierten Programme durch unterstützte.

- Entschlüsseln Sie alle durch Kaspersky Endpoint Security für Windows auf verwalteten Windows-Geräten verschlüsselten Daten (auf Festplatten- oder Dateiebene) und deaktivieren Sie die Verschlüsselungsfunktion auf den verwalteten Geräten entweder lokal oder mittels Programmrichtlinie. 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 Security Center Cloud Console unterstützt maximal 25.000 verwaltete Geräte pro Administrationsserver.

Um eine Migration auf Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 den Richtungspfeil (>) 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 Security Center Cloud Console 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 Security Center Cloud Console unterstützt werden, klicken Sie auf den entsprechenden Link. Dieser öffnet in der Online-Hilfe einen Abschnitt mit einer Liste verwalteter Programme, die von Kaspersky Security Center Cloud Console unterstützt werden.

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

7. Die Liste der standardmäßig exportierten Gruppenobjekte anzeigen. Bei Bedarf können Sie auch Nicht-Gruppenobjekte 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 globalen Aufgaben der verwalteten Programme 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 Security Center Cloud Console 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:

- Administrationsgruppenstruktur, 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 Programme

  Richtlinien des Administrationsservers und des Administrationsagenten werden nicht exportiert.

- Gruppenaufgaben der ausgewählten verwalteten Programme 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console.

10. Nach Abschluss des Imports zeigt der Migrationsassistent eine Liste der Installationspakete des Administrationsagenten an, die in Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console verwalten können. Wechseln Sie dazu nach **Geräte** → **Verwaltete 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 Security Center Cloud Console. 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 Security Center Cloud Console. 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 Security Center Cloud Console 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 für die Programmversionen, die von Kaspersky Security Center Cloud Console unterstützt werden.
- Um aktuelle Richtlinien zu verwenden, aktualisieren Sie die Web-Plug-ins, für die Programme, die Sie durch Kaspersky Security Center Cloud Console verwalten möchten.

- Deinstallieren Sie Kaspersky-Programme, die von Kaspersky Security Center Cloud Console nicht unterstützt werden, von den verwalteten Geräten und ersetzen Sie anschließend die deinstallierten Programme durch unterstützte.

Kaspersky Security Center Cloud Console unterstützt maximal 25.000 verwaltete Geräte pro Administrationsserver.

Schritte der Migration

Die Migration auf Kaspersky Security Center Cloud Console 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 Security Center Cloud Console, 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 Security Center Cloud Console verwaltet.
- Alle Objekteinstellungen, die vor der Migration wirksam waren, sind erhalten geblieben.

Szenario: Rückmigration von Kaspersky Security Center Cloud Console auf Kaspersky Security Center

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

Erforderliche Vorrausetzungen

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

- Kaspersky Security Center Cloud Console 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 diese 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 Security Center Cloud Console entweder entspricht oder aktueller ist.

2. **Erstellen eines benutzerdefinierten Installationspakets in Kaspersky Security Center Cloud Console**

   Wechseln Sie zu Kaspersky Security Center Cloud Console 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 **Befehlszeilenparameter der ausführbaren Datei** den Schlüssel `-s` an.

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

   Bleiben Sie in Kaspersky Security Center Cloud Console und erstellen Sie eine Aufgabe zur Remote-Installation unter Verwendung des benutzerdefinierten Installationspakets, dass 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 Security Center Cloud Console verwaltet wurden, werden jetzt durch den lokal ausgeführten Kaspersky Security Center Administrationsserver verwaltet.
- Die Geräte werden automatisch in die Administrationsgruppe verschoben, die in den Einstellungen des Installationspakets angegeben wurde.

Die Aufgabe zur Remote-Installation kann in Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console unterstützt werden.

Migrationsszenario

Das Szenario verläuft in den folgenden Schritten:

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

   Wechseln Sie zu Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console statt.

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

   Die folgenden Archivtypen werden unterstützt:.zip, .cab, .tar und .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 Security Center Cloud Console übernimmt deren Verwaltung.

   Alle Geräte werden nach Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console.

Über den Schnellstartassistenten

Mit dem Schnellstartassistenten von Kaspersky Security Center Cloud Console können Sie die minimal erforderlichen Aufgaben und Richtlinien erstellen, eine Mindestauswahl an Einstellungen anpassen und mit dem Erstellen von Installationspaketen für Kaspersky-Programme beginnen. Im Assistenten können Sie die folgenden Änderungen an Kaspersky Security Center Cloud Console vornehmen:

- Das Herunterladen von Installationspaketen für verwaltete Kaspersky-Programme 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-Programme in der Liste **Gerätesuche und Softwareverteilung** → **Softwareverteilung 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 Security Center Cloud Console fordert Sie automatisch zur Ausführung des Schnellstartassistenten auf, nachdem Sie einen Unternehmensarbeitsbereich erstellt und Kaspersky Security Center Cloud Console zum ersten Mal gestartet haben. Sie können den Schnellstartassistenten auch jederzeit manuell starten.

Den Schnellstartassistent ausführen

Kaspersky Security Center Cloud Console fordert Sie automatisch zur Ausführung des Schnellstartassistenten auf, nachdem Sie einen Unternehmensarbeitsbereich erstellt und Kaspersky Security Center Cloud Console 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 das Einstellungen-Symbol ( ) neben dem Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

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

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

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

Der Assistent fordert Sie auf, die Erstkonfiguration von Kaspersky Security Center Cloud Console durchzuführen. Folgen Sie den Anweisungen 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-Programme aus der Liste aus. Für die ausgewählten Programme erstellt Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console

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 akzeptiere die Nutzungsbedingungen für Kaspersky Security Network**

  Kaspersky Security Center Cloud Console 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 Nutzungsbedingungen für Kaspersky Security Network ab**

  Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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-Programme

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-Programme

- Ein autonomes Installationspaket für den Administrationsagenten erstellen

  Dieses Paket werden Sie für die Installation des Administrationsagenten auf den Verteilungspunkten verwenden. Kaspersky Security Center Cloud Console 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. Sie können den Fortschritt auf der Registerkarte **In Bearbeitung ()** des Abschnitts **Installationspakete** verfolgen (**Gerätesuche und Softwareverteilung → Softwareverteilung und Zuweisung → Installationspakete**).

  Zu Authentifizierungszwecken wird jedes autonome Installationspaket unter Verwendung eines Zertifikats signiert. Das Zertifikat wird regelmäßig neu ausgestellt. Nach jeder erneuten Ausstellung eines Zertifikats aktualisiert Kaspersky Security Center Cloud Console 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.

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-Programmen.

Erstbereitstellung von Kaspersky-Anwendungen

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

Szenario: Erstmalige Bereitstellung von Kaspersky-Programmen

Dieses Szenario beschreibt die Installation von Kaspersky-Programmen auf Client-Geräten mittels Kaspersky Security Center Cloud Console. 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-Programme auf den vernetzten Geräten bereitstellen.

Wenn das Szenario abgeschlossen ist, werden die Kaspersky-Programme auf den ausgewählten Client-Geräten im Netzwerk Ihrer Organisation bereitgestellt. Sie können all diese Geräte mit installierten Kaspersky-Programmen 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.
- In den Firewall-Ausnahmen der verwalteten Geräte ist folgende Adresse enthalten: https://aes.s.kaspersky-labs.com/endpoints.
- Sie besitzen Informationen zu den Interneteinstellungen für die Client-Geräte in Ihrer Organisation, zu den Gateways und zu den Einstellungen des Proxyservers.

Schritte

Die Erstbereitstellung von Kaspersky-Programmen erfolgt schrittweise:

1. **Ein Gerät als Verteilungspunkt auswählen**

   In Kaspersky Security Center Cloud Console 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.

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-Programme 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-Programmen beginnen.

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

   Erstellen Sie Aufgaben, um den Administrationsagenten und verwaltete Kaspersky-Programme auf den Client-Geräten im Netzwerk Ihrer Organisation zu installieren. Verwenden Sie beim Erstellen der Aufgaben den Aufgabentyp **Remote-Installation eines Programms**. 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-Programme 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-Programmen ausgeführt werden.

   Optional können Sie eine Aufgabe zur Remote-Installation erstellen, um den Administrationsagenten und verwaltete Kaspersky-Programme 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-Programmen 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 autonomes 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-Programme 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-Programmen 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-Programme** generieren und anzeigen. Stellen Sie sicher, dass die verwalteten Kaspersky-Programme auf allen Client-Geräten in Ihrer Organisation installiert sind.

Für die vollständige Festplattenverschlüsselung wird von Kaspersky Security Center Cloud Console nur BitLocker unterstützt.

Erstellen von Installationspaketen für Kaspersky-Programme

Um Programme von Kaspersky auf vernetzten Geräten in Ihrem Unternehmen bereitzustellen, müssen Sie Installationspakete für Kaspersky-Programme in Kaspersky Security Center Cloud Console erstellen.

So erstellen Sie ein Installationspaket für ein Kaspersky-Programm:

1. Führen Sie eine der folgenden Aktionen aus:

   - Wechseln Sie im Hauptmenü zu **Gerätesuche und Softwareverteilung → Softwareverteilung 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 auf der ersten Seite des Assistenten die Option **Installationspaket für ein Programm von Kaspersky erstellen** aus.

   Eine Liste der auf den Kaspersky-Webservern verfügbaren Programmpakete wird angezeigt.

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.

   Der Download des Installationspakets beginnt. Sie können das Fenster des Assistenten schließen, oder mit dem nächsten Schritt der Anleitung fortfahren. Wenn sie das Fenster des Assistenten schließen, wird der Download im Hintergrund fortgesetzt.

   Um den Fortschritt des Downloadvorgangs des Installationspakets zu verfolgen:

   a. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Datenverwaltung** → **Installationspakete** → **In Bearbeitung ()**.

   b. Sie können den Fortschritt in den Spalten **Download-Fortschritt** und **Download-Status** der Tabelle verfolgen.

   Wenn der Vorgang abgeschlossen ist, wird das Installationspaket der Liste auf der Registerkarte **Heruntergeladen** hinzugefügt. Wenn der Downloadvorgang anhält und der Downloadstatus zu **EULA akzeptieren** wechselt, klicken Sie auf den Namen des Installationspakets und fahren Sie mit dem nächsten Schritt der Anleitung fort.

   Wenn Sie planen, eine Migration von Kaspersky Security Center Web Console auf Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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. Bei einigen Programmen von Kaspersky wird während des Downloads die Schaltfläche **EULA anzeigen** angezeigt. Wird diese angezeigt, gehen Sie wie folgt vor:

   a. Klicken Sie auf die Schaltfläche **EULA anzeigen**, um den Endbenutzer-Lizenzvertrag (EULA) zu lesen.

   b. Lesen Sie die EULA, die auf dem Bildschirm angezeigt wird, und klicken Sie erneut auf Schaltfläche **Akzeptieren**.

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

7. Klicken Sie nach Abschluss des Downloads auf **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.

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 Weisen:

   - Wenn Sie die Aufgabe für sekundäre Administrationsserver einer gewählten Administrationsgruppe erstellen möchten, starten Sie das Erstellen einer Gruppenaufgabe für diese Gruppe.

   - Wenn Sie die Aufgabe für eine Auswahl der sekundären Administrationsserver erstellen möchten, starten Sie das Erstellen einer Aufgabe für eine Reihe von Geräten.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

   Wählen Sie im 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 Security Center Cloud Console 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 Security Center Cloud Console 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.

Zu Authentifizierungszwecken wird jedes autonome Installationspaket unter Verwendung eines Zertifikats signiert. Das Zertifikat wird regelmäßig neu ausgestellt. Nach jeder erneuten Ausstellung eines Zertifikats aktualisiert Kaspersky Security Center Cloud Console 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.

So erstellen Sie ein autonomes Installationspaket:

1. Führen Sie eine der folgenden Aktionen aus:

   - Wechseln Sie im Hauptmenü zu **Gerätesuche und Softwareverteilung → Softwareverteilung 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 **Verteilen**.

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 auf der ersten Seite des Assistenten sicher, dass die Option **Administrationsagent gemeinsam mit diesem Programm installieren** aktiviert ist, wenn Sie den Administrationsagenten zusammen mit dem ausgewählten Programm installieren möchten.

   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 das ausgewählte Programm 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 dasselbe Programm erneut erstellen möchten. Das autonome Installationspaket wird im selben Ordner abgelegt.

7. Standardmäßig ist auf der Seite **In die Liste mit verwalteten Geräten verschieben** des Assistenten 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 diese 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 auf der nächsten Seite des Assistenten 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 der autonomen Installationspakete angezeigt, die Sie aufrufen können.

Anzeigen der Liste der autonomen Installationspakete

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:

   - Wechseln Sie im Hauptmenü zu **Gerätesuche und Softwareverteilung → Softwareverteilung 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.
- **Dateihash**. 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:

- 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 regelmäßig neu ausgestellt. Nach jeder erneuten Ausstellung eines Zertifikats aktualisiert Kaspersky Security Center Cloud Console 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.

- Löschen Sie ein autonomes Installationspaket, indem Sie auf die Schaltfläche **Entfernen** 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 Security Center Cloud Console 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.

So erstellen Sie ein benutzerdefiniertes Installationspaket:

1. Führen Sie eine der folgenden Aktionen aus:

   - Wechseln Sie im Hauptmenü zu **Gerätesuche und Softwareverteilung → Softwareverteilung 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 auf der ersten Seite des Assistenten die Option **Installationspaket aus einer Datei erstellen** aus.

4. Geben Sie auf der nächsten Seite des Assistenten den Namen des Installationspakets an und klicken Sie auf **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 Security Center Cloud Console heruntergeladen.

   Wenn der Administrationsserver feststellt, dass das Archiv ein Kaspersky-Programm enthält, wird eine Fehlermeldung angezeigt. Sie können Installationspakete für Kaspersky-Programme von den Kaspersky-Webservern herunterladen. Dieser Vorgang steht unter **Vorgänge → Programme von Kaspersky → Aktuelle Programmversionen** zur Verfügung.

6. Wenn die ausgewählte Archivdatei mehrere ausführbare Dateien enthält, wählen Sie auf der nächsten Seite des Assistenten jene 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 Security Center Cloud Console ist die Gesamtgröße aller Installationspakete auf dem Administrationsserver auf 500 MB begrenzt. Wenn beim Erstellen eines Installationspakets die zulässige Gesamtgröße überschritten wird, löschen Sie die zuvor erstellten 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.
- **Quelle**. Der Programmhersteller.
- **Programm**. Das im benutzerdefinierten Installationspaket enthaltene Programm.
- **Version**. Programmversion.
- **Sprache**. Sprache des Programms, das im benutzerdefinierten Installationspaket enthalten ist.
- **Größe (MB)**. Größe des benutzerdefinierten Installationspakets.
- **Betriebssystem**. Betriebssystem, für welches das benutzerdefinierte Installationspaket erstellt wurde.
- **Erstellt**. Erstellungsdatum des Installationspaketes.
- **Geändert**. Änderungsdatum des Installationspaketes.
- **Typ**. Kaspersky-Programm oder Drittanbieter-Programm.

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.
- Festplatte: SSD 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.

Richtlinieneinstellungen des Administrationsagenten

Gehen Sie folgendermaßen vor, um die Richtlinieneinstellungen des Administrationsagenten anzupassen:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Richtlinien und Profile**.
2. Klicken Sie auf den Namen der Richtlinie für Administrationsagenten.

   Das Eigenschaftenfenster der Richtlinie des Administrationsagenten wird geöffnet.

Bedenken Sie, dass für Geräte auf Basis von Windows, macOS oder Linux jeweils unterschiedliche Einstellungen zur Verfügung stehen.

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 **Einstellungen erben** können Sie Einstellungen für die Vererbung der Richtlinie anpassen:
  - **Einstellungen aus übergeordneter Richtlinie erben**

    Ist diese Option aktiviert, so werden die Werte der Richtlinieneinstellungen aus der Richtlinie der obersten Hierarchie-Ebene vererbt und können nicht geändert werden.

    Diese Option ist standardmäßig aktiviert.

  - **Vererben der Einstellungen für untergeordnete Richtlinien erzwingen**

    Ist diese Option aktiviert, so werden die folgenden Aktionen ausgeführt, nachdem die Richtlinienänderungen übernommen wurden:
    - Einstellungen der Richtlinie werden in die Tochter-Richtlinien, d.h. in die Richtlinien der untergeordneten Administrationsgruppen, übertragen.
    - Im Block **Einstellungen erben** des Abschnitts **Allgemein** im Eigenschaftenfenster aller untergeordneten Richtlinien wird die Option **Einstellungen aus Richtlinie der höheren Ebene erben** automatisch aktiviert.

    Ist diese Option aktiviert, so können die Einstellungen der untergeordneten Richtlinien nicht geändert werden.

    Diese Option ist standardmäßig deaktiviert.

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 Programmeinstellungen

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)**
- Dem Programm ist es erlaubt, auf dem Gerät erweiterte Daten über Richtlinien zu erfassen

Der Administrationsagent, der auf einem verwalteten Gerät installiert ist, überträgt Informationen über die angewendete Sicherheitsanwendungs-Richtlinie an die Sicherheitsanwendung (z. B. Kaspersky Endpoint Security für Windows). Die übertragenen Informationen können Sie auf der Benutzeroberfläche der Sicherheitsanwendung einsehen.

Der Administrationsagent überträgt die folgenden Informationen:

- Zeit, zu der die Richtlinie dem verwalteten Gerät zugestellt wurde
- Name der aktiven Richtlinie oder der Richtlinie für mobile Benutzer, als die Richtlinie an das verwaltete Gerät zugestellt wurde
- 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

  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 die Aufgabe zur Remote-Deinstallation des Administrationsagenten angeben. Klicken Sie dazu auf die Schaltfläche **Ändern**.

  Diese Option ist standardmäßig deaktiviert.

Datenverwaltung

Im Abschnitt **Datenverwaltung** können Sie die Objekttypen auswählen, deren Daten vom Administrationsagenten an den Administrationsserver übertragen werden sollen. Wenn das Ändern der in diesem Abschnitt angegebenen Einstellungen in der Richtlinie des Administrationsagenten unterbunden ist, können Sie diese Einstellungen nicht ändern. Die Einstellungen im Abschnitt **Datenverwaltung** sind nur auf Geräten verfügbar, die unter Windows laufen:

- **Informationen über installierte Programme**
- **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 zu Schwachstellen in Programmen und entsprechenden Updates

  Wenn diese Option aktiviert ist, werden Informationen über Schwachstellen in Drittherstellerr-Anwendungen (Microsoft-Software eingeschlossen), die auf verwalteten Geräten erkannt wurden, sowie Informationen über Software-Updates zum Beheben der Drittherstellerr-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 von Microsoft-Software 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:

- Unter **Benutzern die Verwaltung von Windows-Updates erlauben** können Sie Windows-Updates beschränken, die Benutzer auf ihren Geräten manuell mithilfe von Windows Update installieren können.

  Wenn auf Windows 10-Geräten der Windows Update-Dienst bereits Updates für das Gerät gefunden hat, wird die neue Option, die Sie unter **Benutzern die Verwaltung von Windows-Updates erlauben** auswählen können, erst angewendet, wenn die gefundenen Updates installiert wurden.

  Wählen Sie ein Element in der Dropdown-Liste:

  - Benutzern die Installation aller anwendbaren Windows-Updates erlauben

Benutzer können alle Microsoft Windows-Updates installieren, die für ihre Geräte anwendbar sind.

Wählen Sie diese Option aus, wenn Sie nicht in die Installation von Updates eingreifen möchten.

Wenn der Benutzer Microsoft Windows-Updates manuell installiert, können die Updates von Microsoft-Servern statt vom Administrationsserver heruntergeladen werden. Dies ist möglich, wenn der Administrationsserver diese Updates noch nicht heruntergeladen hat. Update-Download von Microsoft-Servern führt zu zusätzlichem Datenverkehr.

- **Benutzern nur die Installation von genehmigten Windows-Updates erlauben**

  Benutzer können alle Microsoft Windows-Updates installieren, die für ihre Geräte anwendbar und die von Ihnen genehmigt sind.

  Beispielsweise können Sie zuerst die Installation von Updates in einer Testumgebung überprüfen und sich vergewissern, dass sie den Betrieb von Geräten nicht stören, und erst dann die Installation dieser genehmigten Updates auf Client-Geräten erlauben.

  Wenn der Benutzer Microsoft Windows-Updates manuell installiert, können die Updates von Microsoft-Servern statt vom Administrationsserver heruntergeladen werden. Dies ist möglich, wenn der Administrationsserver diese Updates noch nicht heruntergeladen hat. Update-Download von Microsoft-Servern führt zu zusätzlichem Datenverkehr.

- **Benutzern die Installation von Windows-Updates nicht erlauben**

  Benutzer können Microsoft Windows-Updates nicht manuell auf Ihren Geräten installieren. Alle anwendbaren Updates werden so installiert, wie sie von Ihnen angepasst wurden.

  Wählen Sie diese Variante aus, wenn Sie die Installation von Updates zentral verwalten möchten.

  Beispielsweise können Sie den Update-Zeitplan so optimieren, dass das Netzwerk nicht überlastet wird. Sie können Updates nach Büroschluss planen, damit sie sich nicht auf die Produktivität der Benutzer auswirken.

- In der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** können Sie den Modus für die Suche nach Updates auswählen:

  - **Aktiv**

    Wenn diese Option aktiviert ist, initiiert der Administrationsserver mit Unterstützung des Administrationsagenten eine Anfrage vom Windows Update-Agent des Client-Geräts zur Update-Quelle: Windows Update Server oder WSUS. Der Administrationsagent überträgt die vom Windows Update-Agent abgerufenen Daten an den Administrationsserver.

    Die Option wird nur wirksam, wenn die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** der Aufgabe *Suche nach 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. Die Einstellungen im Abschnitt **Verwaltung des Neustarts** sind nur auf Geräten verfügbar, die unter Windows laufen:

- **Betriebssystem nicht neu starten**

  Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Für das Abschließen des Vorgangs ist es erforderlich, ein Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten) neu zu starten. Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für die 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, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

- **Benutzer fragen**

Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und fordert den Benutzer auf, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterten Einstellungen definiert werden: Text der Nachricht für den Benutzer, die Anzeigehäufigkeit der Nachricht, sowie die Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, an denen Benutzer in der Lage sein müssen, den passendsten 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. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

  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 das Neustarten des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einer Textverarbeitungsanwendung bearbeitet wird und nicht gespeichert wurde, erlaubt die Anwendung keinen Neustart des Geräts.

  Wenn diese Option aktiviert ist, wird das Schließen solcher Anwendungen auf einem gesperrten Gerät erzwungen, bevor das Gerät neu gestartet wird. Das kann dazu führen, dass Benutzer ihre nicht gespeicherten 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 Security Center Cloud Console

Das Audit des Administrators ist unter folgenden Bedingungen verfügbar:

- Die Lizenz für das Schwachstellen- und Patch-Management wird verwendet
- Der Administrator verfügt über die Berechtigung zum Start der Desktopfreigabe auf dem Remote-Gerät

Wenn diese Option deaktiviert ist, dann ist das Audit des Administrators auf dem Remote-Gerät deaktiviert.

Diese Option ist standardmäßig deaktiviert.

- **Masken für die Dateien, die bei Lesezugriff überwacht werden sollen**

  Diese Liste enthält Dateimasken. Wenn das Audit aktiviert ist, verfolgt das Programm, welche Dateien der entsprechenden Masken vom Administrator gelesen werden, und speichert Informationen über das Lesen von Dateien. Die Liste ist verfügbar, wenn das Kontrollkästchen **Audit aktivieren** aktiviert ist. Die Dateimasken können geändert und neue Masken zur Liste hinzugefügt werden. Neue Dateimasken müssen in der Liste in einer neuen Zeile hinzugefügt werden.

  Standardmäßig sind die Dateimasken *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf angegeben.

- **Masken für die Dateien, deren Bearbeitung überwacht werden soll**

  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**

- **Zeitplan der Verbindung**

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, wird ein für den Betrieb des Administrationsagenten erforderlicher UDP-Port zur Liste der Ausschlüsse der Microsoft Windows-Firewall hinzugefügt.

    Diese Option ist standardmäßig aktiviert.

  - Verbindungs-Gateway auf 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 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. Der standardmäßige UDP-Port für die Verbindung zum KSN-Proxyserver ist 15111.

- 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 **Push-Server ausführen** 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 **Zeitplan der Verbindung** 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 **Zeitplan der Verbindung** 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 Abfrage festlegen** und **Zeitplan für vollständige Abfrage festlegen** eingerichtet wurde.

  Wenn diese Option deaktiviert ist, fragt der Administrationsserver das Netzwerk nicht ab.

  Diese Option ist standardmäßig aktiviert.

- 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.

- Active Directory

  Wenn diese Option aktiviert ist, fragt der Verteilungspunkt automatisch das Active Directory ab und richtet sich dabei nach dem Zeitplan, der über den Link **Abfragezeitplan festlegen** eingerichtet wurde.

  Wenn diese Option deaktiviert ist, fragt der Verteilungspunkt Active Directory nicht ab.

  Diese Option ist standardmäßig aktiviert.

Netzwerk-Einstellungen für Verteilungspunkte

Im Abschnitt **Netzwerk-Einstellungen für Verteilungspunkte** können Sie die Einstellungen für den Internetzugang festlegen:

- **Proxyserver verwenden**
- **Adresse**
- **Port**
- Proxyserver für lokale Adressen umgehen

  Wenn die Option aktiviert ist, wird bei der Verbindung mit den Geräten im lokalen Netzwerk kein Proxyserver verwendet.

  Diese Option ist standardmäßig deaktiviert.

- Authentifizierung am Proxyserver

  Wenn das Kästchen aktiviert ist, können Sie in den Eingabefeldern Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Benutzername**
- **Kennwort**

KSN Proxy (Verteilungspunkte)

Im Abschnitt **KSN Proxy (Verteilungspunkte)** können Sie 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. Standardmäßig befindet sich die KSN-Erklärung unter %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

Diese Option ist standardmäßig deaktiviert. Die Aktivierung dieser Option wird erst wirksam, wenn die Option **Ich akzeptiere die Nutzungsbedingungen für 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 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. Der standardmäßige UDP-Port für die Verbindung zum KSN-Proxyserver ist 15111.

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	✓	–	–
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 → Verbindungsprofile	✓	–	–
Konnektivität → Zeitplan der Verbindung	✓	✓	✓
Netzwerkabfrage durch Verteilungspunkte	✓	–	–
Netzwerk-Einstellungen für Verteilungspunkte	✓	✓	✓
KSN Proxy (Verteilungspunkte)	✓	–	✓

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:

   - Wechseln Sie im Hauptmenü zu **Gerätesuche und Softwareverteilung → Softwareverteilung 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:

- 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 vom Administrationsagenten verwendeten UDP-Ports zur Liste der Ausschlüsse der Microsoft Windows Firewall hinzugefügt.

  Diese Option ist standardmäßig aktiviert.

- **Keinen Proxyserver verwenden**
- **Proxyserver verwenden**

  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.

Erweitert

Im Abschnitt **Erweitert** können Sie konfigurieren, wie das Verbindungs-Gateway verwendet wird:

- **Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway herstellen**
- **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.

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 Security Center Cloud Console 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 Security Center Cloud Console vorgesehen werden, der für die virtuellen Maschinen von geringem Wert ist.

Bei der Installation des Administrationsagenten auf einer virtuellen Maschine oder einer Vorlage, aus der virtuelle Maschinen erstellt werden sollen, ist es empfehlenswert, wie folgt vorzugehen:

- Wenn eine Remote-Installation ausgeführt wird, wählen Sie im Eigenschaftenfenster für das Installationspaket des Administrationsagenten im Abschnitt **Erweitert** die Option **Einstellungen für VDI optimieren** aus.
- Wenn mithilfe des Assistenten eine interaktive Installation ausgeführt wird, wählen Sie im Fenster des Assistenten die Option **Einstellungen des Administrationsagenten für die virtuelle Infrastruktur optimieren** aus.

Durch Auswählen der Optionen werden die Einstellungen des Administrationsagenten so geändert, dass standardmäßig die folgenden Funktionen deaktiviert werden (bevor eine Richtlinie angewendet wird):

- Informationen über die installierte Software empfangen
- Informationen über die Hardware empfangen
- Informationen über vorhandene Schwachstellen empfangen
- Informationen über erforderliche Updates empfangen

Üblicherweise müssen die aufgezählten Funktionen auf den virtuellen Maschinen nicht aktiviert sein, damit die Software und die virtuelle Hardware darauf einheitlich sind.

Das Deaktivieren der Funktionen kann rückgängig gemacht werden. Wenn eine der deaktivierten Funktionen doch erforderlich ist, kann sie mithilfe der Richtlinie des Administrationsagenten oder in den lokalen Einstellungen des Administrationsagenten aktiviert werden. Die lokalen Einstellungen des Administrationsagenten sind über das Kontextmenü des entsprechenden Geräts in der Verwaltungskonsole verfügbar.

Unterstützung von dynamischen virtuellen Maschinen

Kaspersky Security Center Cloud Console 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 Datenbank des Administrationsservers hinzugefügt. Nach dem Deaktivieren dieser virtuellen Maschine muss der sie betreffende Eintrag auch aus der Datenbank des Administrationsservers gelöscht werden.

Damit die Funktionalität des automatischen Löschens der Einträge über virtuelle Maschinen bei der Installation des Administrationsagenten auf der Vorlage, aus der die dynamischen virtuellen Maschinen erstellt werden, funktioniert, muss die Option **Dynamischen Modus für VDI aktivieren** aktiviert werden:

- Im Falle einer Remote-Installation im Eigenschaftenfenster des Installationspakets des Administrationsagenten (Abschnitt **Erweitert**)

- Für die interaktive Installation – im Installationsassistenten des Administrationsagenten

Die Option **Dynamischen Modus für VDI aktivieren** muss bei der Installation des Administrationsagenten auf realen Geräten nicht aktiviert werden.

Wenn es erforderlich ist, dass Ereignisse auf dynamischen virtuellen Maschinen eine bestimmte Zeit nach dem Löschen der Maschinen auf dem Administrationsserver gespeichert werden, muss im Eigenschaftenfenster des Administrationsservers im Abschnitt **Ereignis-Datenverwaltung** die Option **Ereignisse von gelöschten Geräten weiterhin speichern** aktiviert und die maximale Speicherdauer der Ereignisse in Tagen angegeben werden.

Unterstützung des Kopierens von virtuellen Maschinen

Kaspersky Security Center Cloud Console 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.

Verwendung des Administrationsagenten für Windows, macOS und Linux: 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	macOS	Linux
Installation			
Automatische Installation von Updates und Patches für den Administrationsagenten	✓	–	–

Automatische Verteilung von Schlüsseln	✓	✓	✓
Installation durch manuelles Starten der Installer der Programme auf den Geräten	✓	✓	✓
Erzwungene Synchronisierung	✓	✓	✓
Verteilungspunkt			
Netzwerkabfrage	✓ • IP-Bereiche abfragen • Windows-Netzwerkabfrage • Abfrage der Active Directory	–	✓ IP-Bereiche abfragen
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 macOS-Verteilungspunkten eine Push-Installation auf Windows-Geräten durchzuführen.	Es ist nicht möglich, mithilfe von Linux-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)	✓	✓	✓
Unterstützung von dynamischen virtuellen Maschinen	✓	✓	✓
Anderes			
Audit von Aktionen auf einem Remote-Client-Gerät mithilfe der Windows Desktopfreigabe	✓	–	–
Verwaltung von Geräteneustarts	✓	–	–
Verbindungsmanager	✓	✓	✓
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 ein Programm 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 **Geräte** → **Aufgaben**.
2. Klicken Sie auf den Namen der Aufgabe zur Remote-Installation, für die Sie die Unix-spezifischen Einstellungen festlegen möchten.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.
3. Gehen Sie zu **Programmeinstellungen** → **Unix-spezifische Einstellungen**.
4. Geben Sie die folgenden Einstellungen an:
   - **Legen Sie ein Kennwort für das Root-Benutzerkonto fest (nur bei Softwareverteilung mittels SSH)**

     Wenn der Befehl `sudo` auf dem Zielgerät nicht verwendet werden kann, ohne das Kennwort anzugeben, wählen Sie diese Option aus und geben Sie dann das Kennwort für das Root-Benutzerkonto an. Kaspersky Security Center Cloud Console überträgt das Kennwort in verschlüsselter Form an das Zielgerät, entschlüsselt das Kennwort und startet dann im Namen des Root-Benutzerkontos mit dem angegebenen Kennwort den Installationsvorgang.

     Kaspersky Security Center Cloud Console verwendet das Benutzerkonto oder das angegebene Kennwort nicht, um eine SSH-Verbindung herzustellen.
   - **Geben Sie den Pfad eines auf dem Zielgerät befindlichen temporären Ordners mit Berechtigungen zur Ausführung von Dateien an (nur bei Softwareverteilung mittels SSH)**

     Wenn das Verzeichnis /tmp auf dem Zielgerät nicht über die Ausführungsberechtigung verfügt, wählen Sie diese Option aus und geben Sie den Pfad des Verzeichnisses mit der Ausführungsberechtigung an. Kaspersky Security Center Cloud Console 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 Security Center Cloud Console ist es möglicherweise erforderlich, Drittanbietersoftware zu löschen, die mit dem zu installierenden Programm nicht kompatibel ist. Kaspersky Security Center Cloud Console bietet mehrere Methoden zur Deinstallation von Drittanbieter-Programmen.

Inkompatible Programme während der Konfiguration der Remote-Installation eines Programms entfernen

Sie können die Option **Inkompatible Programme automatisch entfernen** aktivieren, wenn Sie die Remote-Installation einer Sicherheitsanwendung konfigurieren. Diese Option finden Sie im Assistenten für die Bereitstellung des Schutzes. Wenn diese Option aktiviert ist, entfernt Kaspersky Security Center Cloud Console inkompatible Programme vor der Installation einer Sicherheitsanwendung auf einem 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 Security Center Cloud Console 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.

Assistent für die Bereitstellung des Schutzes

Um Programme von Kaspersky zu installieren, können Sie den Assistenten für die Bereitstellung des Schutzes verwenden. Der Assistent für die Bereitstellung des Schutzes ermöglicht die Remote-Installation von Programmen 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 Softwareverteilung → Softwareverteilung und Zuweisung → Installationspakete**. Dieses Installationspaket kann zur weiteren Installation des Programms herangezogen werden.

- Erstellen und starten eine Aufgabe zur Remote-Installation für eine Reihe von Geräten oder für eine Administrationsgruppe. Die soeben erstellte Aufgabe zur Remote-Installation wird in dem Abschnitt **Aufgaben** gespeichert. Sie können diese Aufgabe später manuell starten. Der Aufgabentyp ist **Remote-Installation eines Programms**.

Assistent für die Bereitstellung des Schutzes starten

So starten Sie den Assistenten für die Bereitstellung des Schutzes manuell:

Wechseln Sie im Hauptmenü zu **Gerätesuche und Softwareverteilung** → **Softwareverteilung 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 1. Auswählen des Installationspakets

Wählen Sie 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 2. Auswählen der Version des Administrationsagenten

Wenn Sie das Installationspaket eines anderen Programms ausgewählt haben (nicht den Administrationsagenten), müssen Sie auch den Administrationsagenten installieren, da dieser das Programm mit dem Kaspersky Security Center Administrationsserver verbindet.

Wählen Sie die aktuellste Version des Administrationsagenten aus.

Schritt 3. Auswählen der Geräte

Geben Sie eine Liste mit Geräte an, auf denen das Programm 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 festlegen.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

Schritt 4. Festlegen der Einstellungen für die Aufgabe zur Remote-Installation

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.

Passen Sie die erweiterte Einstellung an:

Programm nicht neu installieren, wenn es bereits installiert ist

Wenn diese Option aktiviert ist, wird das ausgewählte Programm nicht neu installiert, wenn es bereits auf dem Client-Gerät installiert ist.

Wenn Sie dieses Kontrollkästchen deaktivieren, wird das Programm in jedem Fall installiert.

Diese Option ist standardmäßig aktiviert.

Schritt 5. 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. Für das Abschließen des Vorgangs ist es erforderlich, ein Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten) neu zu starten. Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für die Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreies Arbeiten kritisch ist.

- **Gerät 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, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und fordert den Benutzer auf, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterten Einstellungen definiert werden: Text der Nachricht für den Benutzer, die Anzeigehäufigkeit der Nachricht, sowie die Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, an denen Benutzer in der Lage sein müssen, den passendsten 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. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

    Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

  - **Neu starten 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 das Neustarten des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einer Textverarbeitungsanwendung bearbeitet wird und nicht gespeichert wurde, erlaubt die Anwendung keinen Neustart des Geräts.

Wenn diese Option aktiviert ist, wird das Schließen solcher Anwendungen auf einem gesperrten Gerät erzwungen, bevor das Gerät neu gestartet wird. Das kann dazu führen, dass Benutzer ihre nicht gespeicherten 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 6. Deinstallieren inkompatibler Programme vor der Installation

Dieser Schritt ist nur dann verfügbar, wenn das zu verteilende Programm bekanntlich mit anderen Programmen inkompatibel ist.

Wählen Sie diese Option, wenn Sie möchten, dass Kaspersky Security Center Cloud Console 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 7. 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 8. 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 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 angeben, um das Programm zu installieren.

  Um das Benutzerkonto anzugeben, unter dem das Installationsprogramm ausgeführt werden soll, klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **Lokales Benutzerkonto** 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.

Schritt 9. 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 Security Center Cloud Console verwendet die folgenden Netzwerkeinstellungen zur Interaktion mit externen Diensten.

Netzwerkeinstellungen

Netzwerkeinstellungen	Adresse	Beschreibung
Port: 443 Protokoll: HTTPS	activation-v2.kaspersky.com/activationservice/activationservice.svc	Aktivierung 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 • Überprüfen der Erreichbarkeit der Kaspersky-Server Vor dem Herunterladen von Kaspersky-Datenbanken und Softwaremodulen überprüft Kaspersky Security Center Cloud Console, ob die Kaspersky-Server erreichbar sind. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet das Programm öffentliche DNS-Server.

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	Verwenden von Kaspersky Security Network
Port: 443, 1443 Protokoll: HTTPS	ksn-a-stat-geo.kaspersky-labs.com 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
Protokoll: HTTPS	click.kaspersky.com	Folgen von Links aus

	redirect.kaspersky.com	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

Verwaltung mobiler Geräte

Die Verwaltung von mobilen Geräten mittels Kaspersky Security Center Cloud Console 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.

Weitere Informationen zur Bereitstellung des Schutzes und Verwaltung für mobile Geräte finden Sie in der Hilfe von Kaspersky Security für mobile Endgeräte.

Möglichkeiten von Detection and Response

Dieser Abschnitt enthält Informationen zu Kaspersky-Lösungen, die in die Kaspersky Security Center Cloud Console integriert werden können, um der Konsole die Funktionen für Detection and Response hinzuzufügen.

Über die Möglichkeiten von Detection and Response

Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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.

Sie können die folgenden Lösungen integrieren:

- Kaspersky Endpoint Detection and Response Optimum

  Nachdem ein Programm aus der Kaspersky Endpoint Protection Platform (auch als EPP bezeichnet) eine Bedrohung erkennt, fügt Kaspersky Security Center Cloud Console 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 Response-Aktionen auswählen, beispielsweise ein nicht vertrauenswürdiges Objekt isolieren, ein kompromittiertes Gerät vom Netzwerk isolieren oder für ein nicht vertrauenswürdiges Objekt eine Regel zur Verhinderung seiner Ausführung 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 Security Center Cloud Console 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

Die folgenden Lösungen von Kaspersky bieten Funktionen für Detection and Response, die in die Benutzeroberfläche von Kaspersky Security Center Cloud Console integriert werden können:

- Kaspersky Endpoint Detection and Response (EDR) Optimum
- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response (EDR) Expert

In der folgenden Tabelle sind die Änderungen aufgeführt, welche die Lösungen nach ihrer Integration an der Benutzeroberfläche von Kaspersky Security Center Cloud Console vornehmen.

Änderungen in der Benutzeroberfläche durch integrierte Kaspersky-Lösungen

Lösung	Änderungen in Kaspersky Security Center Cloud Console
Kaspersky EDR Optimum	Fügt die folgenden Elemente hinzu: • Abschnitt **Alarme** (**Überwachung und Berichterstattung** → **Alarme**). Die von dieser Lösung erkannten Alarme werden auf der Registerkarte **Optimum** angezeigt. • Ein Widget auf für das **Dashboard** (**Überwachung und Berichterstattung** → **Dashboard**).
Kaspersky MDR	Fügt die folgenden Elemente hinzu: • Den Abschnitt **MDR** (**Überwachung und Berichterstattung** → **MDR**). • Die Option **Funktionen von MDR anzeigen** (**Einstellungen** → **Einstellungen der Benutzeroberfläche** → **Funktionen von MDR anzeigen**). • Ein Widget auf für das **Dashboard** (**Überwachung und Berichterstattung** → **Dashboard**).
Kaspersky EDR Expert	Fügt die folgenden Elemente hinzu: • Abschnitt **Alarme** (**Überwachung und Berichterstattung** → **Alarme**). Die von dieser Lösung erkannten Alarme werden auf der Registerkarte **Expert** angezeigt. • Abschnitt **Vorfälle** (**Überwachung und Berichterstattung** → **Vorfälle**). • Abschnitt **Bedrohungssuche** (**Überwachung und Berichterstattung** → **Threat Hunting**). • Abschnitt **Benutzerdefinierte Regeln** (**Überwachung und Berichterstattung** → **Benutzerdefinierte Regeln**). • Allgemeine Einstellungen von Kaspersky EDR Expert (**Einstellungen** → **Integration** → **Kaspersky EDR Expert**). • Widgets für das **Dashboard** (**Überwachung und Berichterstattung** → **Dashboard**).

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 Security Center Cloud Console ermöglicht eine Suche der Geräte auf der Grundlage der angegebenen Kriterien. Sie können Suchergebnisse in einer Textdatei speichern.

Mit der Such- und Ermittlungsfunktion können folgende Geräte gefunden werden:

- Verwaltete Geräte der Administrationsgruppen des Kaspersky Security Center Cloud Console Administrationsservers und seiner sekundären Administrationsserver.
- Nicht zugeordnete Geräte, die vom Kaspersky Security Center Cloud Console Administrationsserver 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 Security Center Cloud Console 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, Active Directory-Abfrage oder IP-Bereichsabfrage. Stellen Sie sicher, dass der Abfragezeitplan den Anforderungen Ihres Unternehmens entspricht.

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 einrichten, dass diese Geräte automatisch in die Gruppe **Verwaltete Geräte** verschoben werden. 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 Security Center Cloud Console durch regelmäßiges Abfragen des Windows-Netzwerks, der IP-Bereiche und der Active Directory in dem Unternehmensnetzwerk. Die Netzwerkabfrage kann entweder manuell oder automatisch nach einem Zeitplan gestartet werden.

Basierend auf den Ergebnissen dieser Abfrage aktualisiert Kaspersky Security Center Cloud Console die Liste der nicht zugeordneten Geräte. Sie können auch Regeln für neu erkannte Geräte konfigurieren, die automatisch in Administrationsgruppen verschoben werden sollen.

Kaspersky Security Center Cloud Console verwendet die folgenden Methoden zur Netzwerkabfrage:

- *IP-Bereiche durchsuchen*. Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Active Directory*. Informationen über Struktur der Active Directory-Einheit und zu den DNS-Namen der Geräte aus Active Directory-Gruppen werden in der Kaspersky Security Center Cloud Console-Datenbank gespeichert.

Die Abfrageergebnisse werden in dem Abschnitt **Gerätesuche und Softwareverteilung** → **Entdeckung** für jede Abfragemethode separat angezeigt.

Ein Gerät kann in mehr als einem Erkennungsbereich angezeigt werden. Wenn ein Gerät in der HQ-Domäne erkannt wird und die Adresse 192.168.0.1 lautet, wird das Gerät sowohl auf der Registerkarte **Windows-Domänen** als auch auf der Registerkarte **IP-Abfrage** 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verteilungspunkte** aus.
3. Klicken Sie auf den Namen des Verteilungspunkts, den Sie zum Abfragen des Netzwerks verwenden möchten.

   Das Eigenschaftenfenster des Verteilungspunkts wird geöffnet.

4. Wählen Sie den Bereich **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.
7. Klicken Sie auf die Schaltfläche **OK**.

Die Eigenschaften werden gespeichert und auf alle entdeckten Windows-Domänen und Arbeitsgruppen angewendet.

Abfrage der Active Directory

Verwenden Sie die Abfrage des Active Directory, wenn Sie Active Directory verwenden – andernfalls wird die Verwendung anderer Arten der Abfrage empfohlen. Wenn Sie Active Directory verwenden, aber einige der vernetzten Geräte nicht als Teilnehmer aufgelistet sind, können diese Geräte nicht mittels Abfrage des Active Directory gefunden werden.

Kaspersky Security Center Cloud Console sendet eine Anfrage an den Domänencontroller und erhält die Gerätestruktur von Active Directory. Die Abfrage des Active Directory wird stündlich durchgeführt.

Einstellungen für die Abfrage des Active Directory anzeigen und ändern

Um die Einstellungen für die Abfrage des Active Directory anzuzeigen und zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

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

5. Passen Sie die folgenden Einstellungen an:

   a. Aktivieren bzw. Deaktivieren der Active Directory-Abfrage mithilfe der Umschalttaste.

   b. Abfragezeitplan ändern.

      Das Standardabfrageintervall beträgt eine Stunde. Alte Daten werden vollständig durch die bei der nächsten Abfrage empfangenen Daten ersetzt.

   c. Konfigurieren Sie erweiterte Einstellungen, um den Abfragungsbereich auszuwählen:

      - Active Directory-Domäne, zu der Kaspersky Security Center Cloud Console gehört
      - Domänengesamtstruktur, zu der Kaspersky Security Center Cloud Console gehört
      - Festgelegte Liste von Active Directory-Domänen

   d. Um eine Domäne zum Abfragebereich hinzuzufügen, klicken Sie auf **Hinzufügen** und legen Sie die Adresse des Domänencontrollers sowie den Namen und das Kennwort des Benutzerkontos für den Zugriff darauf fest.

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

Die neuen Einstellungen werden auf die Active Directory-Abfrage angewendet.

Ergebnisse der Abfrage des Active Directory anzeigen

Um die Ergebnisse der Abfrage des Active Directory anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Softwareverteilung → Entdeckung → Active Directory**.

   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 Security Center Cloud Console 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 Security Center Cloud Console-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 Security Center Cloud Console 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 Security Center Cloud Console das Netzwerk 192.168.0.0/24 automatisch zur Liste der Abfrageadressen hinzu. Kaspersky Security Center Cloud Console 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

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

3. Klicken Sie auf den Namen des Verteilungspunkts, den Sie zum Abfragen des Netzwerks verwenden möchten.

   Das Eigenschaftenfenster des Verteilungspunkts wird geöffnet.

4. Wählen Sie den Bereich **IP-Bereiche** 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.

IP-Bereich hinzufügen und bearbeiten

Ursprünglich erhält Kaspersky Security Center Cloud Console 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 Security Center Cloud Console das Netzwerk 192.168.0.0/24 automatisch zur Liste der Abfrageadressen hinzu. Kaspersky Security Center Cloud Console 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

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

3. Klicken Sie auf den Namen des Verteilungspunkts, den Sie zum Abfragen des Netzwerks verwenden möchten.

   Das Eigenschaftenfenster des Verteilungspunkts wird geöffnet.

4. Wählen Sie den Bereich **IP-Bereiche** 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 Security Center Cloud Console 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.

Berechnung der Anzahl und Konfiguration der Verteilungspunkte

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:

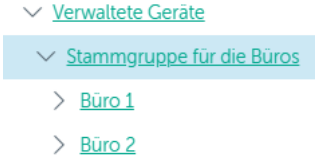
- Aufbau der Struktur der Administrationsgruppen unter Berücksichtigung der Netztopologie. Die Struktur der Administrationsgruppen muss die Netztopologie nicht unbedingt genau widerspiegeln. Es ist ausreichend, wenn den einzelnen Teilen des Netzwerkes bestimmte Administrationsgruppen entsprechen.

- 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 Security Center Cloud Console 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

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

3. Klicken Sie auf 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.

  - **Multicast verwenden**

    Wenn diese Option aktiviert ist, werden die Installationspakete automatisch mithilfe von IP-Multicasting an die Client-Geräte innerhalb einer Gruppe verteilt.

    IP-Multicasting erhöht die Dauer für die Installation eines Programms aus einem Installationspaket in eine Gruppe von Client-Geräten. Dagegen reduziert es die Installationsdauer, wenn Sie ein Programm auf einem einzelnen Client-Gerät installieren.

  - **Adresse für IP-Multicast**

    IP-Adresse, die für das Multicasting verwendet wird. Die IP-Adresse kann man im Bereich 224.0.0.0 – 239.255.255.255 festgelegt werden.

    Standardmäßig weist Kaspersky Security Center Cloud Console 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.

  - **Updates verteilen**

    Aus den folgenden Quellen werden Updates an verwaltete Geräte verteilt:

    - Von diesen Verteilungspunkt, wenn diese Option aktiviert ist.
    - Von anderen Verteilungspunkten, dem Administrationsserver oder Kaspersky-Update-Servern, wenn diese Option deaktiviert ist.

    Wenn Sie zur Bereitstellung von Updates Verteilungspunkte verwenden, können Sie Datenverkehr sparen, da Sie die Anzahl der Downloads reduzieren. Außerdem können Sie den Administrationsserver entlasten und die Last auf die Verteilungspunkten verlegen. Um den Datenverkehr und die Last zu optimieren, können Sie die Anzahl der Verteilungspunkte für Ihr Netzwerk berechnen.

    Wenn Sie diese Option deaktivieren, kann sich die Anzahl der Update-Downloads und die Belastung des Administrationsservers erhöhen. Diese Option ist standardmäßig aktiviert.

  - **Installationspakete verteilen**

Aus den folgenden Quellen werden Installationspakete an verwaltete Geräte verteilt:

- Von diesen Verteilungspunkt, wenn diese Option aktiviert ist.
- Von anderen Verteilungspunkten, dem Administrationsserver oder Kaspersky-Update-Servern, wenn diese Option deaktiviert ist.

Wenn Sie zur Bereitstellung von Installationspaketen Verteilungspunkte verwenden, können Sie Datenverkehr sparen, da Sie die Anzahl der Downloads reduzieren. Außerdem können Sie den Administrationsserver entlasten und die Last auf die Verteilungspunkten verlegen. Um den Datenverkehr und die Last zu optimieren, können Sie die Anzahl der Verteilungspunkte für Ihr Netzwerk berechnen.

Wenn Sie diese Option deaktivieren, kann sich die Anzahl der Downloads von Installationspaketen und die Belastung des Administrationsservers erhöhen. Diese Option ist standardmäßig aktiviert.

- **Push-Server ausführen**

  In Kaspersky Security Center Cloud Console 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 Netzwerkspeicherort).

  Nur Geräte unter der Verwaltung von Windows können ihren Netzwerkspeicherort ermitteln. Die Bestimmung des Netzwerkspeicherorts ist für Geräte unter der Verwaltung anderer Betriebssysteme nicht verfügbar.

- Im Abschnitt **KSN Proxy** können Sie das Programm anpassen, um den Verteilungspunkt zum Weiterleiten von KSN-Anfragen von den verwalteten Geräten zu verwenden:

  KSN Proxy auf 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. Standardmäßig befindet sich die KSN-Erklärung unter %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

Diese Option ist standardmäßig deaktiviert. Die Aktivierung dieser Option wird erst wirksam, wenn die Option **Ich akzeptiere die Nutzungsbedingungen für 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.

- Passen Sie die Einstellungen für die Abfrage der Windows-Domänen, des Active Directory oder des IP-Bereichs für den Verteilungspunkt an:

  - Windows-Domänen

    Sie können für Windows-Domänen die Gerätesuche erlauben und den Zeitplan für die Abfrage festlegen.

  - Active Directory

    Sie können für Active Directory die Netzwerkabfrage erlauben und den Zeitplan für die Abfrage festlegen.

    Wenn Sie das Kontrollkästchen **Abfrage des Active Directory erlauben** aktivieren, 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.

  - IP-Bereiche

    Sie können die Gerätesuche für IPv4-Bereiche und IPv6-Netzwerke aktivieren.

    Wenn Sie die Option **Abfrage des Bereichs zulassen** aktivieren, können Sie zu untersuchende Bereiche hinzufügen und den Zeitplan für sie festlegen. Sie können IP-Bereich zur Liste der untersuchten Bereiche hinzufügen.

    Wenn Sie die Option **Zeroconf zum Abfragen von IPv6-Netzwerken verwenden** aktiviert haben, fragt der Verteilungspunkt das IPv6-Netzwerk automatisch unter Verwendung von Zero-configuration Networking (auch als *Zeroconf* bezeichnet) ab. In diesem Fall werden angegebene IP-Bereiche ignoriert, da der Verteilungspunkt das gesamte Netzwerk abfragt. Für Verteilungspunkte mit Linux ist die Option **Zeroconf zum Abfragen von IPv6-Netzwerken verwenden** verfügbar. Um die Zeroconf IPv6-Abfrage verwenden zu können, müssen Sie das Tool "avahi-browser" auf dem Verteilungspunkt installieren.

- Geben Sie im Abschnitt **Erweitert** den Ordner an, den der Verteilungspunkt zum Speichern der zu verteilenden Daten verwenden soll:

  - **Standardordner verwenden**

    Bei Auswahl dieser Option wird zum Speichern der Ordner auf dem Verteilungspunkt verwendet, in dem der Administrationsagent installiert wurde.

  - **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.

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 **Geräte** → **Gruppen**.
2. Wählen Sie in der Struktur der Administrationsgruppe die Administrationsgruppe aus, für welche Sie die zugewiesenen Verteilungspunkte ansehen möchten.
3. Klicken Sie auf die Registerkarte **Verteilungspunkte**.
4. Fügen Sie mithilfe der Schaltfläche **Zuweisen** neue Verteilungspunkte zur Administrationsgruppe hinzu oder löschen Sie zugewiesene Verteilungspunkte mithilfe der Schaltfläche **Zuweisen aufheben**.

Je nach Ihren Änderungen werden neue Verteilungspunkte zur Liste hinzugefügt oder bestehende Verteilungspunkte daraus entfernt.

Verteilungspunkt als Push-Server verwenden

In Kaspersky Security Center Cloud Console 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

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

3. Klicken Sie auf den 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 **Push-Server ausführen**.

   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.

   > Um eine Verbindung zwischen dem als Push-Server fungierenden Verteilungspunkt und einem verwalteten Gerät herzustellen, müssen Sie den angegebenen Push-Server-Port manuell zur Ausschlussliste der Microsoft Windows-Firewall hinzufügen.

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 **Push-Server ausführen** 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 Security Center Cloud Console 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 direkt auf den Administrationsserver zugreift (d. h. nicht über einen Verteilungspunkt):

     a. Wechseln Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte**.

     b. Klicken Sie 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. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

     Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

     b. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **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 **Geräte** → **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 **Geräte** → **Gruppenhierarchie**.
2. Klicken Sie auf die Schaltfläche **Importieren**.

   Daraufhin wird der Assistent für das Erstellen einer Administrationsgruppenstruktur gestartet. Folgen Sie den Anweisungen des Assistenten.

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 **Geräte** → **Verschiebungsregeln**.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

3. Geben Sie im nächsten Fenster auf der Registerkarte **Allgemein** die folgenden Informationen an:

   - **Regelname**

     Geben Sie einen Namen für die neue Regel ein.

     Wenn Sie eine Regel kopieren, erhält die neue Regel denselben Namen wie die ursprüngliche Regel, aber der Name wird um einen Index im Format () erweitert – z. B. (1).

   - **Administrationsgruppe**

     Wählen Sie die Administrationsgruppe aus, in welche die Geräte automatisch verschoben werden sollen.

   - **Aktive Regel**

     Wenn diese Option aktiviert ist, wird die Regel aktiviert und ab dem Speicherzeitpunkt berücksichtigt.

     Wenn diese Option deaktiviert ist, wird die Regel erstellt, aber nicht aktiviert. Sie wird erst berücksichtigt, sobald Sie diese Option aktivieren.

   - **Nur Geräte verschieben, die keiner Administrationsgruppe angehören**

     Wenn diese Option aktiviert ist, werden nur nicht zugeordnete Geräte in die ausgewählte Gruppe verschoben.

     Wenn diese Option deaktiviert ist, werden Geräte, die bereits zu anderen Administrationsgruppen gehören, sowie nicht zugeordnete Geräte in die ausgewählte Gruppe verschoben.

   - **Ausführung der Regel**

     Sie können eine der folgenden Varianten auswählen:

     - **Pro Gerät einmal ausführen**

       Die Regel wird für jedes Gerät, das Ihren Kriterien entspricht, einmal ausgeführt.

     - **Pro Gerät einmal 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. Geben Sie auf der Registerkarte **Regelbedingungen** mindestens ein Kriterium an, nach dem die Geräte in eine Administrationsgruppe verschoben werden.

5. Klicken Sie auf die Schaltfläche **Speichern**.

Die Verschiebungsregel wird erstellt. Sie wird in der Liste der Verschiebungsregeln angezeigt.

Je höher ihre Position in der Liste ist, desto höher ist die Priorität der Regel. Um die Priorität einer Verschiebungsregel zu erhöhen oder zu verringern, verschieben Sie die Regel mit der Maus in der Liste nach oben bzw. nach unten.

Wenn die 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).

Kopieren von Regeln für das Verschieben von Geräten

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 **Geräte** → **Verschiebungsregeln**.
   - Wechseln Sie im Hauptmenü zu **Gerätesuche und Softwareverteilung** → **Softwareverteilung und Zuweisung** → **Verschiebungsregeln**.

   Die Liste mit Verschiebungsregeln wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen neben der Regel, die Sie kopieren möchten.
3. Klicken Sie auf die Schaltfläche **Kopieren**.
4. Passen Sie im nächsten Fenster die folgenden Informationen auf der Registerkarte **Allgemein** an oder belassen Sie diese, wie sie sind, wenn Sie die Regel unverändert kopieren möchten:

   - **Regelname**

     Geben Sie einen Namen für die neue Regel ein.

     Wenn Sie eine Regel kopieren, erhält die neue Regel denselben Namen wie die ursprüngliche Regel, aber der Name wird um einen Index im Format () erweitert – z. B. (1).

   - **Administrationsgruppe**

     Wählen Sie die Administrationsgruppe aus, in welche die Geräte automatisch verschoben werden sollen.

   - **Aktive Regel**

     Wenn diese Option aktiviert ist, wird die Regel aktiviert und ab dem Speicherzeitpunkt berücksichtigt.

     Wenn diese Option deaktiviert ist, wird die Regel erstellt, aber nicht aktiviert. Sie wird erst berücksichtigt, sobald Sie diese Option aktivieren.

   - **Nur Geräte verschieben, die keiner Administrationsgruppe angehören**

Wenn diese Option aktiviert ist, werden nur nicht zugeordnete Geräte in die ausgewählte Gruppe verschoben.

Wenn diese Option deaktiviert ist, werden Geräte, die bereits zu anderen Administrationsgruppen gehören, sowie nicht zugeordnete Geräte in die ausgewählte Gruppe verschoben.

- Ausführung der Regel

  Sie können eine der folgenden Varianten auswählen:

  - **Pro Gerät einmal ausführen**

    Die Regel wird für jedes Gerät, das Ihren Kriterien entspricht, einmal ausgeführt.

  - **Pro Gerät einmal 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. Geben Sie auf der Registerkarte **Regelbedingungen** mindestens ein Kriterium für die Geräte an, 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.

Manuelles Hinzufügen von Geräten zu einer Administrationsgruppe

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. Wechseln Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte**.
2. Klicken Sie auf den Link **Aktueller Pfad:** `<aktueller Pfad>` über der Liste.
3. Wählen Sie im nächsten Fenster die Administrationsgruppe aus, zu der Sie die Geräte hinzufügen möchten.
4. Klicken Sie auf die Schaltfläche **Geräte hinzufügen**.

   Daraufhin wird der Assistent zum Verschieben von Geräten gestartet.
5. Erstellen Sie eine Liste mit Geräten, die Sie der Administrationsgruppe hinzufügen möchten.

Sie können nur Geräte hinzufügen, deren Informationen bereits durch Anschließen des Geräts oder nach einer Gerätesuche in die Datenbank des Administrationsservers 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.
  - 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: , \ / * ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

6. Zeigen Sie die Liste der Geräte an, die der Administrationsgruppe hinzugefügt werden sollen. Sie können die Liste bearbeiten, indem Sie Geräte hinzufügen oder entfernen.
7. Wenn Sie sichergestellt haben, dass die Liste korrekt ist, klicken Sie auf die Schaltfläche **Weiter**.

Der Assistent verarbeitet die Geräteliste und zeigt das Ergebnis an. Erfolgreich verarbeitete Geräte werden der Administrationsgruppe hinzugefügt und in der Geräteliste mit den Namen angezeigt, die der Administrationsserver bestimmt hat.

Manuelles Verschieben von Geräten oder Clustern in eine Administrationsgruppe

Sie können Geräte aus einer Administrationsgruppe in eine andere verschieben oder von der Gruppe nicht zugeordnete Geräte in eine Administrationsgruppe verschieben.

Sie können auch Cluster oder Server-Arrays von einer Administrationsgruppe in eine andere verschieben. Wenn Sie ein Cluster oder Server-Array in eine andere Gruppe verschieben, werden alle ihre Knoten mit verschoben, da ein Cluster und alle seine Knoten immer derselben Administrationsgruppe angehören. Wenn Sie auf der Registerkarte **Geräte** einen Cluster auswählen, wird die Schaltfläche **In Gruppe verschieben** inaktiv.

So verschieben Sie ein oder mehrere Geräte oder Cluster in eine ausgewählte Administrationsgruppe:

1. Öffnen Sie die Administrationsgruppe, aus welcher Sie die Geräte verschieben möchten. Führen Sie dazu eine der folgenden Aktionen aus:

- Um eine Administrationsgruppe zu öffnen, wechseln Sie im Hauptmenü zu **Geräte** → **Gruppen** → **<Gruppenname>** → **Verwaltete Geräte**.

- Um die Gruppe **Nicht zugeordnete Geräte** im Hauptmenü zu öffnen, wechseln Sie zu **Gerätesuche und Softwareverteilung** → **Nicht zugeordnete Geräte**.

2. Wenn die Administrationsgruppe Cluster oder Server-Arrays enthält, wird der Abschnitt **Verwaltete Geräte** in zwei Registerkarten unterteilt – **Geräte** und **Cluster und Server-Arrays**. Öffnen Sie die Registerkarte für diese Art von Objekt, die Sie verschieben möchten.

3. Aktivieren Sie die Kontrollkästchen neben den Geräten oder Clustern, die Sie in eine andere Gruppe verschieben möchten.

4. Klicken Sie auf die Schaltfläche **In Gruppe verschieben**.

5. Aktivieren Sie in der Hierarchie der Verwaltungsgruppen das Kontrollkästchen neben der Administrationsgruppe, in welche Sie die ausgewählten Geräte oder Cluster verschieben möchten.

6. Klicken Sie auf die Schaltfläche **Verschieben**.

Die ausgewählten Geräte oder Cluster werden in die gewählte Administrationsgruppe verschoben.

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 Softwareverteilung** → **Entdeckung** → **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 und Sie diese ausschließlich manuell löschen. 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 Softwareverteilung** → **Entdeckung** → **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 mehr als (Tage)**

  Wenn diese Option aktiviert ist, können Sie das Zeitintervall festlegen, nach dem das Geräte automatisch aus der Gruppe gelöscht wird. Standardmäßig wird diese Option auch an die untergeordneten Gruppen weitergegeben. Standardmäßig beträgt das Zeitintervall 7 Tage.

  Diese Option ist standardmäßig aktiviert.

- **Aus übergeordneter Gruppe erben**

  Wenn diese Option aktiviert ist, wird der Aufbewahrungszeitraum für die Geräte in der aktuellen Gruppe von der übergeordneten Gruppe geerbt und kann nicht geändert werden.

  Diese Option ist nur für untergeordnete Gruppen verfügbar.

  Diese Option ist standardmäßig aktiviert.

- **Vererben für untergeordnete Gruppen erzwingen**

  Die Einstellungswerte werden an untergeordnete Gruppen verteilt, aber in den Eigenschaften der untergeordneten Gruppen sind diese Einstellungen gesperrt.

  Diese Option ist standardmäßig deaktiviert.

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

Ihre Änderungen werden gespeichert und übernommen.

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 Security Center Cloud Console 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-Programme**

   Zur Konfiguration und Verteilung der Einstellungen für auf den verwalteten Geräten installierte Kaspersky-Programme 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-Programmen 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 *Suche nach Schwachstellen und erforderlichen Updates*

   Erstellen Sie bei Bedarf zusätzliche Aufgaben, um die auf den Client-Geräten installierten Kaspersky-Programme zu verwalten.

3. **Ereignismenge für Datenbank einschätzen und einschränken**

Informationen über Ereignisse in der Funktionsweise der verwalteten Programme werden vom Client-Gerät übertragen und in der Datenbank des Administrationsservers 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.

Ergebnisse

Nach Abschluss dieses Szenarios wird Ihr Netzwerk dank der Konfiguration von Kaspersky-Programmen, den Aufgaben und der vom Administrationsserver empfangenen Ereignissen geschützt sein.

- Die Kaspersky-Programme werden entsprechend den Richtlinien und Richtlinienprofilen konfiguriert.
- Die Programme werden über eine Reihe von Aufgaben verwaltet.
- Die maximale Anzahl der Ereignisse, die in der Datenbank gespeichert werden können, ist eingestellt.

Wenn der Netzwerkschutz angepasst ist, können Sie mit der Konfiguration von regelmäßigen Updates für die Kaspersky-Datenbanken und -Programme fortfahren.

Geräteorientierte und benutzerorientierte Methode der Sicherheitsverwaltung

Sie können die Sicherheitseinstellungen unter Berücksichtigung der Gerätefunktionen oder der Benutzerrollen verwalten. Die erste Methode wird *geräteorientierte Sicherheitsverwaltung* genannt, die zweite *benutzerorientierte Sicherheitsverwaltung*. Um verschiedene Programmeinstellungen auf verschiedene Geräte anzuwenden, können Sie eine dieser Verwaltungsmethoden oder eine Kombination aus beiden Methoden verwenden.

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 Programmeinstellungen zuweisen. Als Ergebnis erhält bei der benutzerorientierten Sicherheitsverwaltung jede Abteilung – die Buchhaltung und die Personalabteilung – eine eigene Konfiguration der Einstellungen für Kaspersky-Programme. Die Konfiguration der Einstellungen legt fest, welche Programmeinstellungen von Benutzern angepasst werden können und welche zwangsweise übernommen und durch den Administrator gesperrt sind.

Bei der benutzerorientierten Sicherheitsverwaltung können Sie einzelnen Benutzern bestimmte Programmeinstellungen zuweisen. Das ist z. B. sinnvoll, wenn ein Mitarbeiter eine besondere Rolle im Unternehmen einnimmt oder wenn Sie Sicherheitsvorfälle überwachen möchten, die auf dem Gerät einer bestimmten Person auftreten. Unter Berücksichtigung der Rolle des Mitarbeiters im Unternehmen können Sie die Berechtigung dieser Person zur Änderung der Programmeinstellungen erweitern oder einschränken. So würden Sie z. B. die Berechtigungen eines Systemadministrators, der Client-Geräte im lokalen Büro verwaltet, erweitern.

Es ist auch eine Kombination der geräteorientierten und der benutzerorientierten Herangehensweise an die Sicherheitsverwaltung möglich. So können Sie zum Beispiel für jede Administrationsgruppe eine bestimmte Programmrichtlinie anpassen und Richtlinienprofile für eine oder mehrere Benutzerrollen Ihres Unternehmens erstellen. In diesem Fall werden die Richtlinien und Richtlinienprofile in der folgenden Reihenfolge angewendet:

1. Es werden Richtlinien angewendet, die für geräteorientierte Sicherheitsverwaltung erstellt wurden.
2. Sie werden mittels Richtlinienprofilen gemäß den Prioritäten der Profile geändert.
3. Die Richtlinien werden von den Richtlinienprofilen geändert, die Benutzerrollen zugewiesen sind.

Einrichtung und Verteilung von Richtlinien: geräteorientierte Herangehensweise

Dieser Abschnitt beschreibt das Szenario der geräteorientierten Herangehensweise an die zentralisierte Konfiguration der Programme von Kaspersky, 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 Programme von Kaspersky umfasst die folgenden Schritte:

1 Programmrichtlinien anpassen

Passen Sie die Einstellungen der auf den verwalteten Geräten installierten Kaspersky-Programme an, indem Sie für jedes Programm eine Richtlinie erstellen. Diese Auswahl an Richtlinien wird an die Client-Geräte weitergegeben.

Wenn Sie den Schutz Ihres Netzwerks im Schnellstartassistenten konfigurieren, erstellt Kaspersky Security Center Cloud Console 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-Programme, 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 Security Center Cloud Console 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-Programme weitergegeben und von ihnen übernommen.

   Sie können überprüfen, ob die Richtlinien und Richtlinienprofile an ein bestimmtes Gerät übertragen wurden. Kaspersky Security Center Cloud Console 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-Programme gemäß den festgelegten Einstellungen konfiguriert und mittels Richtlinienhierarchie weitergegeben.

Die konfigurierten Programmrichtlinien und Richtlinienprofile werden automatisch auf neue Geräte angewendet, die zu den Administrationsgruppen hinzugefügt werden.

Einrichtung und Verteilung von Richtlinien: benutzerorientierte Herangehensweise

Dieser Abschnitt beschreibt das Szenario der benutzerorientierten Herangehensweise an die zentralisierte Konfiguration der Programme von Kaspersky, 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 Programme von Kaspersky umfasst die folgenden Schritte:

1. **Programmrichtlinien anpassen**

Passen Sie die Einstellungen der auf den verwalteten Geräten installierten Kaspersky-Programme an, indem Sie für jedes Programm eine Richtlinie erstellen. Diese Auswahl an Richtlinien wird an die Client-Geräte weitergegeben.

Wenn Sie den Schutz Ihres Netzwerks im Schnellstartassistenten konfigurieren, erstellt Kaspersky Security Center Cloud Console 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 Programmeinstellungen 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 Programme 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-Programme angewendet, die auf den Benutzergeräten installiert sind.

   Anleitung: Verbinden von Richtlinienprofilen mit Rollen

8. **Richtlinien und Richtlinienprofile an die verwalteten Geräte weitergeben**

   Kaspersky Security Center Cloud Console 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-Programme weitergegeben und von ihnen übernommen.

   Sie können überprüfen, ob die Richtlinien und Richtlinienprofile an ein bestimmtes Gerät übertragen wurden. Kaspersky Security Center Cloud Console registriert das Datum und die Uhrzeit der Weitergabe in den Eigenschaften des Geräts.

   Anleitung: Erzwungene Synchronisierung

Ergebnisse

Nach Abschluss des benutzerorientierten Szenarios werden die Programme von Kaspersky 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 Programmrichtlinien und Richtlinienprofile werden automatisch auf die Geräte dieses Benutzers angewendet.

Manuelle Konfiguration der Richtlinie für Kaspersky Endpoint Security

Dieser Abschnitt enthält Empfehlungen zur Konfiguration der Richtlinie von Kaspersky Endpoint Security. Sie können die Einrichtung im Fenster mit den Richtlinieneigenschaften durchführen. Klicken Sie beim Bearbeiten einer Einstellung auf das Schloss-Symbol rechts neben der entsprechenden Gruppe der Einstellungen, um die angegebenen Werte auf eine Workstation anzuwenden.

Kaspersky Security Network konfigurieren

Kaspersky Security Network (KSN) ist eine Infrastruktur aus Cloud-Diensten, die Informationen über die Reputation von Dateien, Webressourcen und Software enthält. Kaspersky Security Network ermöglicht es Kaspersky Endpoint Security für Windows, schneller auf verschiedenste Bedrohungstypen zu reagieren, verbessert die Leistung der Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen. Weitere Informationen zu Kaspersky Security Network finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows.

Sie können Kaspersky Security Network im Eigenschaftenfenster der Richtlinie von Kaspersky Endpoint Security für Windows im Abschnitt **Programmeinstellungen** → **Erweiterter Schutz** konfigurieren.

So geben Sie die empfohlenen KSN-Einstellungen ein:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie von Kaspersky Endpoint Security für Windows.

   Das Eigenschaftenfenster der gewählten Richtlinie wird geöffnet.
3. Wechseln Sie in den Richtlinieneigenschaften zu **Programmeinstellungen** → **Erweiterter Schutz** → **Kaspersky Security Network**.

4. Stellen Sie sicher, dass die Option **Administrationsserver als KSN-Proxyserver verwenden** aktiviert ist. Diese Option unterstützt Sie bei der Umverteilung und Optimierung des Datenverkehrs im Netzwerk.

   Wenn Sie Managed Detection and Response verwenden, müssen Sie die Option **KSN Proxy** für den Verteilungspunkt aktivieren.

5. Aktivieren Sie bei Bedarf die Verwendung von KSN-Servern, wenn der KSN Proxy-Service nicht verfügbar ist. Aktivieren Sie dazu die Option **Kaspersky Security Network-Server verwenden, wenn der KSN-Proxyserver nicht verfügbar ist**.

   KSN-Server können sich sowohl auf der Seite von Kaspersky (wenn KSN verwendet wird) als auch auf der Seite von Dritten (wenn KPSN verwendet wird) befinden.

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

Die empfohlenen KSN-Einstellungen werden angegeben.

Liste der durch die Firewall geschützten Netzwerke überprüfen

Stellen Sie sicher, dass die Firewall von Kaspersky Endpoint Security für Windows alle Ihre Netzwerke schützt. Standardmäßig schützt die Firewall Netzwerke mit den folgenden Verbindungstypen:

- **Öffentliches Netzwerk**. Antiviren-Programme, Firewalls oder Filter schützen die Geräte in einem solchen Netzwerk nicht.
- **Lokales Netzwerk**. Der Zugriff auf Dateien und Drucker ist für Geräte in diesem Netzwerk eingeschränkt.
- **Vertrauenswürdiges Netzwerk**. Geräte in einem solchen Netzwerk sind vor Angriffen und unbefugtem Zugriff auf Dateien und Daten geschützt.

Wenn Sie ein benutzerdefiniertes Netzwerk konfiguriert haben, stellen Sie sicher, dass es durch die Firewall geschützt wird. Überprüfen Sie dazu die Liste der Netzwerke in den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows. In der Liste werden möglicherweise nicht alle Netzwerke angezeigt.

Weitere Informationen zur Firewall finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows.

Um die Liste der Netzwerke zu überprüfen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte → Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie von Kaspersky Endpoint Security für Windows.

   Das Eigenschaftenfenster der gewählten Richtlinie wird geöffnet.

3. Wechseln Sie in den Richtlinieneigenschaften zu **Programmeinstellungen → Basisschutz → Firewall**.
4. Klicken Sie unter **Verfügbare Netzwerke** auf den Link **Netzwerkeinstellungen**.

   Das Fenster **Netzwerkverbindungen** wird geöffnet. In diesem Fenster wird die Liste der Netzwerke angezeigt.

5. Wenn die Liste ein fehlendes Netzwerk enthält, fügen Sie es hinzu.

Programminformationen aus dem Speicher des Administrationsservers ausschließen

Es wird empfohlen, dass der Administrationsserver keine Informationen über Programm-Module speichert, die auf den Netzwerkgeräten gestartet wurden. Dadurch wird der Speicher des Administrationsservers nicht überlastet.

Sie können das Speichern dieser Information in der Richtlinie von Kaspersky Endpoint Security für Windows deaktivieren.

Um das Speichern von Informationen über installierte Programm-Module zu deaktivieren:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie von Kaspersky Endpoint Security für Windows.

   Das Eigenschaftenfenster der gewählten Richtlinie wird geöffnet.
3. Wechseln Sie in den Richtlinieneigenschaften zu **Programmeinstellungen** → **Allgemeine Einstellungen** → **Berichte und Speicher**.
4. Deaktivieren Sie das Kontrollkästchen **Über die ausgeführten Programme**, unter **Datenübertragung an den Administrationsserver**, wenn diese in der übergeordneten Richtlinie noch aktiviert ist.

   Wenn dieses Kontrollkästchen aktiviert ist, werden in der Datenbank des Administrationsservers Informationen über alle Versionen aller Programm-Module auf den Geräten im Unternehmensnetzwerk gespeichert. Diese Informationen können in der Datenbank von Kaspersky Security Center Cloud Console eine erhebliche Größe (mehrere Gigabyte) einnehmen.

Informationen über installierte Programm-Module werden nicht länger in der Datenbank des Administrationsservers gespeichert.

Wichtige Ereignisse von Richtlinien in der Datenbank des Administrationsservers speichern

Um einen Überlauf der Datenbank des Administrationsservers zu vermeiden, empfehlen wir Ihnen, nur wichtige Ereignisse in der Datenbank zu speichern.

So konfigurieren Sie die Registrierung wichtiger Ereignisse in der Datenbank des Administrationsservers:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie von Kaspersky Endpoint Security für Windows.

   Das Eigenschaftenfenster der gewählten Richtlinie wird geöffnet.
3. Wechseln Sie in den Eigenschaften für Richtlinien zur Registerkarte **Konfiguration von Ereignissen**.
4. Klicken Sie im Abschnitt **Kritisch** auf **Ereignis hinzufügen** und aktivieren Sie die Kontrollkästchen neben den folgenden Ereignissen:

   - *Verletzung des Endbenutzer-Lizenzvertrags*

- *Autostart des Programms ist deaktiviert*
- *Aktivierungsfehler*
- *Aktive Bedrohung gefunden. Erweiterte Desinfektion sollte ausgeführt werden*
- *Desinfektion nicht möglich*
- *Früher geöffneter gefährlicher Link gefunden*
- *Prozess beendet*
- *Netzwerkaktivität verboten*
- *Netzwerkangriff gefunden*
- *Anwendungsstart verboten*
- *Zugriff verweigert (Lokale Datenbanken)*
- *Zugriff verweigert (KSN)*
- *Lokaler Update-Fehler*
- *Der Start von zwei Aufgaben gleichzeitig ist unmöglich*
- *Fehler bei der Interaktion mit Kaspersky Security Center*
- *Nicht alle Komponenten aktualisiert*
- *Fehler beim Übernehmen der Verschlüsselungs- bzw. Entschlüsselungsregeln der Dateien*
- *Fehler bei der Aktivierung des portablen Modus*
- *Fehler bei der Deaktivierung des portablen Modus*
- *Das Verschlüsselungsmodul konnte nicht geladen werden*
- *Richtlinie kann nicht übernommen werden*
- *Fehler beim Ändern der Programmkomponenten*

5. Klicken Sie auf die Schaltfläche **OK**.
6. Klicken Sie im Abschnitt **Funktionsfehler** auf **Ereignis hinzufügen** und aktivieren Sie ausschließlich das Kontrollkästchen neben dem Ereignis *Ungültige Aufgabeneinstellungen. Aufgabeneinstellungen nicht übernommen*.
7. Klicken Sie auf die Schaltfläche **OK**.
8. Klicken Sie im Abschnitt **Warnung** auf **Ereignis hinzufügen** und aktivieren Sie die Kontrollkästchen neben den folgenden Ereignissen:
   - *Selbstschutz des Programms wurde deaktiviert*
   - *Schutzkomponenten sind deaktiviert*

- *Reserveschlüssel ist ungültig*
- *Legitime Software, die von Eindringlingen zur Beeinträchtigung Ihres Computers bzw. Ihrer persönlichen Daten missbraucht werden kann, wurde gefunden (lokale Datenbanken)*
- *Legitime Software, die von Eindringlingen zur Beeinträchtigung Ihres Computers bzw. Ihrer persönlichen Daten missbraucht werden kann, wurde gefunden (KSN)*
- *Objekt gelöscht*
- *Objekt desinfiziert*
- *Der Benutzer hat die Verschlüsselungsrichtlinie abgelehnt*
- *Die Datei wurde vom Administrator aus der Quarantäne auf dem Server von Kaspersky Anti Targeted Attack Platform wiederhergestellt*
- *Die Datei wurde vom Administrator auf dem Server von Kaspersky Anti Targeted Attack Platform in die Quarantäne verschoben*
- *Nachricht beim Verbot des Anwendungsstarts an den Administrator*
- *Nachricht beim Verbot des Zugriffs auf das Gerät an den Administrator*
- *Nachricht beim Verbot des Zugriffes auf eine Webseite an den Administrator*

9. Klicken Sie auf die Schaltfläche **OK**.
10. Klicken Sie im Abschnitt **Information** auf **Ereignis hinzufügen** und aktivieren Sie die Kontrollkästchen neben den folgenden Ereignissen:
    - *Eine Backup-Kopie des Objekts wurde erstellt*
    - *Der Start der Anwendung ist im Testbetrieb untersagt*
11. Klicken Sie auf die Schaltfläche **OK**.

Die Registrierung wichtiger Ereignisse in der Datenbank des Administrationsservers ist konfiguriert.

Manuelle Konfiguration der Gruppenaufgabe zum Update von Kaspersky Endpoint Security

Der optimale und empfohlene Zeitplan für Kaspersky Endpoint Security ist **Nach dem Download von Updates in die Datenverwaltung**, wenn das Kontrollkästchen **Automatische zufällige Verzögerung für Aufgabenstarts verwenden** aktiviert ist.

Aufgaben

In diesem Abschnitt werden Aufgaben beschrieben, die von Kaspersky Security Center Cloud Console verwendet werden.

Über Aufgaben

Kaspersky Security Center Cloud Console 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 Datenbank des Administrationsservers 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 festlegen.

  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 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

So erstellen Sie eine Aufgabe:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **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.

Aufgabenliste anzeigen

Sie können die Liste der Aufgaben anzeigen, die in Kaspersky Security Center Cloud Console erstellt wurden.

Um die Liste der Aufgaben anzuzeigen:

Wechseln Sie im Hauptmenü zu **Geräte** → **Aufgaben**.

Die Aufgabenliste wird angezeigt. Die Aufgaben sind nach den Namen der Programme gruppiert, auf die sie sich beziehen. Beispiele: Die Aufgabe "Remote-Deinstallation eines Programms" bezieht sich auf den Administrationsserver, und die Aufgabe "Suche nach Schwachstellen und erforderlichen Updates" bezieht sich auf den Administrationsagenten.

Um die Eigenschaften einer Aufgabe anzuzeigen,

Klicken Sie auf den Namen der Aufgabe.

Das Fenster mit den Aufgabeneigenschaften enthält mehrere benannte Registerkarten. Zum Beispiel wird der **Aufgabentyp** auf der Registerkarte **Allgemein** angezeigt und der Aufgabenzeitplan auf der Registerkarte **Zeitplan**.

Manuelles Starten einer Aufgabe

Die Anwendung startet Aufgaben gemäß den Zeitplaneinstellungen, die in den Eigenschaften der einzelnen Aufgaben angegeben sind. Sie können die Aufgabe jederzeit manuell starten.

So starten Sie eine Aufgabe manuell:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Aufgaben**.
2. Aktivieren Sie in der Aufgabenliste das Kontrollkästchen neben der Aufgabe, die Sie starten möchten.
3. Klicken Sie auf die Schaltfläche **Starten**.

Die Aufgabe wird gestartet. Sie können den Status der Aufgabe in der Spalte **Status** oder durch Anklicken der Schaltfläche **Ergebnis** überprüfen.

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 festlegen oder eine neue erstellen.

Sie können diese Option beispielsweise zum Starten einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die in einer bestimmten Administrationsgruppe enthalten sind.

- **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 festlegen.

  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, unter dem das Programm installiert und gestartet wurde, dass diese Aufgabe ausführt.

    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. Für das Abschließen des Vorgangs ist es erforderlich, ein Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten) neu zu starten. Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für die Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreies Arbeiten kritisch ist.

- **Gerät 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, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und fordert den Benutzer auf, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterten Einstellungen definiert werden: Text der Nachricht für den Benutzer, die Anzeigehäufigkeit der Nachricht, sowie die Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, an denen Benutzer in der Lage sein müssen, den passendsten 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. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

  Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neu starten 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 das Neustarten des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einer Textverarbeitungsanwendung bearbeitet wird und nicht gespeichert wurde, erlaubt die Anwendung keinen Neustart des Geräts.

Wenn diese Option aktiviert ist, wird das Schließen solcher Anwendungen auf einem gesperrten Gerät erzwungen, bevor das Gerät neu gestartet wird. Das kann dazu führen, dass Benutzer ihre nicht gespeicherten 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:
  - **Einstellung Start nach Zeitplan:**
    - **Manuell**

      Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

      Diese Option ist standardmäßig aktiviert.

- **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.

  Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit alle sechs Stunden ausgeführt.

- **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 Security Center Cloud Console 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, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig sind keine Tage des Monats ausgewählt; die Standardstartzeit ist 18:00:00 Uhr.

- **Nach dem Download von Updates in die Datenverwaltung**

  Wenn neue Updates in die Datenverwaltungen der Verteilungspunkte heruntergeladen wurden, führt Kaspersky Security Center Cloud Console 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 Security Center Cloud Console auf diesem Gerät alle Aufgaben aus, die dies als Zeitplan eingestellt haben. Diese Aufgaben werden stündlich ausgeführt, bis neue Updates gefunden wurden. Kaspersky Security Center Cloud Console 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 Programmtypen aus, die Virenangriffe überwachen. Es sind folgende Programmtypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Programmtypen ausgewählt.

  Sie können abhängig vom Anti-Virus-Programmtyp, der einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Programmtypen, die Sie nicht benötigen.

- **Nach Beenden einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Sie können auswählen, wie die vorherige Aufgabe abgeschlossen werden muss (erfolgreich oder mit Fehler), um den Start der aktuellen Aufgabe auszulösen. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem sie abgeschlossen ist, die *Aufgabe zur Untersuchung auf Viren* ausführen.

- **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 des Programms von Kaspersky 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.

  Ist diese Option deaktiviert, so werden auf den Client-Geräten nur Aufgaben nach Zeitplan ausgeführt, aber für **Manuell**, **Einmal** und **Sofort** werden Aufgaben nur auf jenen Client-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 aktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

  Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

- **Vor dem Aufgabenstart die Geräte mittels Wake-On-LAN hochfahren (Min.)**

  Das Betriebssystem auf dem Gerät startet zum angegebenen Zeitpunkt, bevor die Aufgabe gestartet wird. Standardmäßig beträgt die Zeitspanne fünf Minuten.

  Aktivieren Sie diese Option, wenn Sie möchten, dass die Aufgabe auf allen Client-Geräten aus dem Aufgabenbereich ausgeführt wird, einschließlich jener Geräte, die ausgeschaltet sind, wenn die Aufgabe gestartet werden soll.

  Wenn das Gerät nach Abschluss der Aufgabe automatisch ausgeschaltet werden soll, aktivieren Sie die Option **Geräte nach Abschluss der Aufgabe herunterfahren**. Die Option befindet sich im selben Fenster.

  Diese Option ist standardmäßig deaktiviert.

- Geräte nach Abschluss der Aufgabe herunterfahren

  Sie können diese Option beispielsweise für eine Aufgabe zur Installation von Updates aktivieren, die Updates für Client-Geräte jeden Freitag nach Geschäftsschluss installiert und diese Geräte dann über das Wochenende abschaltet.

  Diese Option ist standardmäßig deaktiviert.

- Aufgabe anhalten, wenn sie länger ausgeführt wird als (Min.)

  Nachdem die festlegte Zeitspanne abgelaufen ist, wird die Aufgabe automatisch angehalten, egal ob sie abgeschlossen ist oder nicht.

  Aktivieren Sie diese Option, wenn Sie Aufgaben, deren Ausführung zu lange dauert, unterbrechen (oder anhalten) möchten.

  Diese Option ist standardmäßig deaktiviert. Die Standardzeit für die Aufgabenausführung beträgt 120 Minuten.

- Benachrichtigungen:
  - Block **Ereignisdaten speichern**:
    - **Alle Ereignisse speichern**
    - **Ereignisse in Bezug auf 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 Security Center Cloud Console 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 **Geräte** → **Aufgaben**.
2. Aktivieren Sie das Kontrollkästchen neben der Aufgabe, die Sie exportieren möchten.

   Sie können nicht mehrere Aufgaben gleichzeitig exportieren. Wenn Sie mehr als eine Aufgabe auswählen, wird die Schaltfläche **Exportieren** deaktiviert. Die Aufgaben des Administrationsservers und die lokalen Aufgaben sind für den Export ebenfalls nicht verfügbar.
3. Klicken Sie auf die Schaltfläche **Exportieren**.
4. Geben Sie im folgenden Fenster **Speichern unter** den Namen und den Pfad der Aufgabendatei an. Klicken Sie auf **Speichern**.

   Das Fenster **Speichern unter** wird nur angezeigt, wenn Sie Google Chrome, Microsoft Edge oder Opera verwenden. Wenn Sie einen anderen Browser verwenden, wird die Aufgabendatei automatisch im Ordner **Downloads** gespeichert.

Aufgaben importieren

Mit Kaspersky Security Center Cloud Console können Sie eine Aufgabe aus einer klt-Datei importieren. Die klt-Datei enthält die exportierte Aufgabe und deren Einstellungen.

Um eine Aufgabe zu importieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Importieren**.
3. Klicken Sie auf die Schaltfläche **Durchsuchen**, um eine Aufgabendatei auszuwählen, die Sie importieren möchten.
4. Geben Sie im folgenden Fenster den Pfad zur klt-Aufgabendatei an und klicken Sie anschließend auf die Schaltfläche **Öffnen**. Beachten Sie, dass Sie nur eine Aufgabendatei auswählen können.

   Die Verarbeitung der Aufgabe beginnt.
5. Nachdem die Aufgabe erfolgreich verarbeitet wurde, wählen Sie die Geräte aus, denen Sie die Aufgabe zuweisen möchten. Wählen Sie dazu eine der folgenden Optionen aus:

- Aufgabe einer Administrationsgruppe zuweisen

  Die Aufgabe wird Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen festlegen oder eine neue erstellen.

  Sie können diese Option beispielsweise zum Starten einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die in einer bestimmten Administrationsgruppe enthalten sind.

- 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. Vielleicht wollen 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 Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen festlegen.

  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 erfolgreichem Import wird die Aufgabe in der Liste der Aufgaben angezeigt. Die Einstellungen und der Zeitplan der Aufgabe werden ebenfalls importiert. Die Aufgabe wird gemäß ihres Zeitplans 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)**.

Verwaltung von Client-Geräten

Dieser Abschnitt beschreibt die Verwaltung von Geräten in den Administrationsgruppen.

Einstellungen des verwalteten Geräts

Um die Einstellungen eines verwalteten Geräts anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte**.

Die Liste der verwalteten Geräte wird angezeigt.

2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des benötigten Geräts.

Das Eigenschaftenfenster des ausgewählten Geräts wird angezeigt.

Allgemein

Der Abschnitt **Allgemein** enthält allgemeine Informationen über das Client-Gerät. Die Informationen beruhen auf Daten, die bei der letzten Synchronisierung des Client-Geräts mit dem Administrationsserver empfangen wurden:

- **Name**

  In diesem Feld lässt sich der Name des Client-Geräts in der Administrationsgruppe anzeigen und ändern.

- **Beschreibung**

  In diesem Feld können Sie eine zusätzliche Beschreibung für das Client-Gerät eingeben.

- **Gruppe**

  Administrationsgruppe, zu der das Client-Gerät gehört.

- **Zuletzt aktualisiert**

  Datum des letzten Updates der Antiviren-Datenbanken oder der Programme auf dem Gerät.

- **Zuletzt im Netzwerk sichtbar**

  Zeitpunkt (Datum und Uhrzeit), zu dem das Gerät zuletzt im Netzwerk gesehen wurde.

- **Verbindung mit dem Administrationsserver**

  Datum und Uhrzeit der letzten Verbindung des auf dem Client-Gerät installierten Administrationsagenten mit dem Administrationsserver.

- **Verbindung mit Administrationsserver nicht trennen**

Wenn diese Option aktiviert ist, wird die dauerhafte Verbindung zwischen dem verwalteten Gerät und dem Administrationsserver aufrecht erhalten. Sie können diese Option verwenden, wenn Sie keine Push-Server einsetzen, die eine solche Verbindung bereitstellen.

Wenn diese Option deaktiviert ist und keine Push-Server verwendet werden, verbindet sich das verwaltete Gerät nur zur Datensynchronisierung oder Datenübertragung mit dem Administrationsserver.

Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

Diese Option ist auf verwalteten Geräten standardmäßig deaktiviert. Diese Option ist auf dem Gerät, auf dem der Administrationsserver installiert ist, standardmäßig aktiviert und bleibt selbst dann aktiviert, wenn Sie versuchen, sie zu deaktivieren.

Netzwerk

Im Abschnitt **Netzwerk** werden Daten zu den Netzwerkeinstellungen des Client-Geräts angezeigt.

- **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.

System

Im Abschnitt **System** werden Daten zum Betriebssystem, das auf dem Client-Gerät installiert ist, angezeigt.

Schutz

Im Abschnitt **Schutz** werden Informationen über den Status des Antiviren-Schutzes auf dem Client-Gerät angezeigt:

- **Gerätestatus**

  Status des Client-Geräts, der ihm anhand der vom Administrator festgelegten Kriterien den Status des Antiviren-Schutzes und der Aktivität des Geräts im Netzwerk zugewiesen wird.

- **Alle Probleme**

  Diese Tabelle enthält eine vollständige Liste mit Problemen, die von den verwalteten Programmen gefunden wurden, die auf dem Client-Gerät installiert sind. Jedes Problem wird von einem Status begleitet, den die Anwendung für dieses Problem vorschlägt, dem Gerät zuzuweisen.

- **Echtzeitschutz**

  Dieses Feld zeigt den aktuellen Status des Echtzeitschutzes auf dem Client-Gerät an.

  Wenn sich der Status auf dem Gerät ändert, wird der neue Status erst im Eigenschaftenfenster des Geräts angezeigt, nachdem das Client-Gerät mit dem Administrationsserver synchronisiert wurde.

- **Letzte Untersuchung auf Befehl**

  Datum und Uhrzeit der letzten Schadsoftware-Untersuchung auf einem Client-Gerät.

- **Gesamtzahl der gefundenen Bedrohungen**

  Gesamtzahl der auf einem Client-Gerät gefundenen Bedrohungen seit der Installation des Antiviren-Programms (seit der ersten Untersuchung des Geräts) oder seit dem letzten Zurücksetzen des Zählers.

- **Aktive Bedrohungen**

  Anzahl der unverarbeiteten Dateien auf einem Client-Gerät.

  In diesem Feld wird die Anzahl der unverarbeiteten Dateien für mobile Geräte 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.

Vom Programm bestimmter Gerätestatus

Im Abschnitt **Gerätestatus wird vom Programm bestimmt** werden Daten über den Gerätestatus, der durch das auf dem Gerät installierte verwaltete Programm bestimmt wird, angezeigt. Der Gerätestatus kann von dem durch Kaspersky Security Center Cloud Console vorgegebenen Status abweichen.

Programme

Im Abschnitt **Programme** wird eine Liste der Kaspersky-Programme angezeigt, die auf dem Client-Gerät installiert sind. Sie können den Programmnamen anklicken, um sich allgemeine Informationen über das Programm, eine Liste mit allen auf dem Gerät aufgetretenen Ereignissen und die Programmeinstellungen anzeigen zu lassen.

Aktive Richtlinien und Richtlinienprofile

Im Abschnitt **Aktive Richtlinien und Richtlinienprofile** werden die derzeit auf dem verwalteten Gerät aktiven Richtlinien und Richtlinienprofile aufgelistet.

Aufgaben

In der Registerkarte **Aufgaben** können Sie die Aufgaben eines Client-Geräts verwalten: Liste der vorhandenen Aufgaben anzeigen, neue Aufgaben erstellen, Aufgaben entfernen, starten und beenden, Aufgabeneinstellungen ändern und die Ergebnisse der Aufgabenausführung anzeigen. Die Aufgabenliste beruht auf Daten, die während der letzten Synchronisierung des Clients mit dem Administrationsserver empfangen wurden. Die Daten über den Aufgabenstatus erhält der Administrationsserver vom Client-Gerät. Sollte keine Verbindung hergestellt sein, erscheint der Status nicht.

Ereignisse

In der Registerkarte **Ereignisse** werden Ereignisse angezeigt, die für das ausgewählte Client-Gerät auf dem Administrationsserver registriert wurden.

Vorfälle

In der Registerkarte **Vorfälle** können Sie Vorfälle für ein Client-Gerät anzeigen, bearbeiten oder erstellen. Vorfälle können sowohl automatisch mithilfe von auf dem Client-Gerät installierten Verwaltungsprogrammen von Kaspersky als auch manuell durch den Administrator erstellt werden. Wenn beispielsweise einige Benutzer immer wieder Schadsoftware von ihrem Wechseldatenträger auf das Gerät übertragen, kann der Administrator einen Vorfall erstellen. Der Administrator kann im Text des Vorfalls eine kurze Beschreibung des Falls bereitstellen und Aktionen vorschlagen (etwa Disziplinarmaßnahmen für 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 Vorfällen kann als Bedingung für die Änderung des Status eines Geräts auf *Kritisch* oder *Warnung* ausgewählt werden.

Dieser Abschnitt enthält eine Liste der für das Gerät erstellten Vorfälle. Die Vorfälle werden nach Signifikanz und Typ eingestuft. Der Vorfalltyp wird vom Kaspersky-Programm, das den Vorfall erstellt hatte, bestimmt. Bearbeitete Vorfälle können in der Liste durch Aktivieren des Kontrollkästchens in der Spalte **Bearbeitet** gekennzeichnet werden.

Tags

In der Registerkarte **Tags** können Sie die Liste der Schlüsselwörter verwalten, auf deren Grundlage die Suche nach Client-Geräten ausgeführt wird: Liste der vorhandenen Tags anzeigen, Tags aus der Liste zuweisen, Regeln für die automatische Zuweisung von Tags konfigurieren, neue Tags hinzufügen und alte Tags umbenennen, sowie Tags löschen.

Programm-Registry

In Abschnitt **Programm-Registry** können Sie die Registry der auf dem Client-Gerät installierten Programme und der Programm-Updates anzeigen lassen und die Darstellung der Programm-Registry konfigurieren.

Die Daten über die installierten Programme sind verfügbar, wenn der auf dem Client-Gerät installierte Administrationsagent die erforderlichen Daten auf den Administrationsserver überträgt. Die Einstellungen für die Übertragung der Informationen auf den Administrationsserver können Sie im Eigenschaftenfenster des Administrationsagenten oder seiner Richtlinie im Abschnitt **Datenverwaltung** anpassen. Informationen über installierte Programme werden nur für Geräte bereitgestellt, die unter Windows laufen.

Der Administrationsagent stellt Informationen über die Programme auf Grundlage der Daten der Systemregistrierung bereit.

- **Nur inkompatible Sicherheitsanwendungen anzeigen**

  Wenn Sie diese Option aktivieren, werden in der Programmliste nur die Sicherheitsanwendungen angezeigt, die mit Kaspersky-Programmen nicht kompatibel sind.

  Diese Option ist standardmäßig deaktiviert.

- **Updates anzeigen**

  Wenn Sie diese Option aktivieren, werden in der Programmliste nicht nur Programme, sondern auch die für die Programme installierten Update-Pakete angezeigt.

  Um die Liste der Updates anzuzeigen, werden 100 KB an Datenverkehr benötigt. Wenn Sie die Liste schließen und wieder öffnen, fallen erneut 100 KB an Datenverkehr an.

  Diese Option ist standardmäßig deaktiviert.

- **In Datei exportieren**

  Klicken Sie auf diese Schaltfläche, um die Liste der Programme, die auf dem Gerät installiert sind, als csv- oder txt-Datei zu exportieren.

- **Verlauf**

  Klicken Sie auf diese Schaltfläche, um Ereignisse anzuzeigen, die sich auf die Installation von Programmen auf dem Gerät beziehen. Folgende Informationen werden angezeigt:

  - Datum und Uhrzeit der Installation des Programms auf dem Gerät
  - Name der Anwendung
  - Anwendungsversion

- **Eigenschaften**

  Klicken Sie auf diese Schaltfläche, um die Eigenschaften des Programms anzuzeigen, das in der Liste der auf dem Gerät installierten Programme ausgewählt wurde. Folgende Informationen werden angezeigt:

  - Name der Anwendung
  - Anwendungsversion
  - Programmhersteller

Ausführbare Dateien

In Abschnitt **Ausführbare Dateien** werden ausführbare Dateien angezeigt, die auf dem Client-Gerät entdeckt wurden.

Verteilungspunkte

In diesem Abschnitt finden Sie eine Liste der Verteilungspunkte, mit denen das Gerät interagiert.

- In Datei exportieren

  Mithilfe der Schaltfläche **In Datei exportieren** können Sie die Liste der Verteilungspunkte, mit denen das Gerät interagiert, in einer Datei speichern. Standardmäßig exportiert das Programm 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

Im Abschnitt **Hardware-Register** finden Sie Informationen zur Hardware, die auf dem Client-Gerät installiert ist. Diese Informationen können Sie für Windows-Geräte und Linux-Geräte anzeigen.

Stellen Sie sicher, dass auf den Linux-Geräten, von denen Sie die Hardware-Details abrufen möchten, das Tool lshw installiert ist. Die von virtuellen Maschinen abgerufene Hardware-Details können je nach verwendetem Hypervisor unvollständig sein.

Verfügbare Updates

In diesem Abschnitt können Sie sich die Liste der auf dem Gerät gefundenen Software-Updates anzeigen lassen, die nicht installiert wurden.

Installierte Updates anzeigen

Ist diese Option aktiviert, werden in der Update-Liste nicht installierte Updates sowie Updates angezeigt, die auf dem Client-Gerät bereits installiert wurden.

Diese Option ist standardmäßig deaktiviert.

Schwachstellen in Programmen

Im Abschnitt **Schwachstellen in Programmen** können Sie sich Informationen über die Schwachstellen von Drittanbietersoftware anzeigen lassen, die auf den Client-Geräten installiert ist. Mithilfe der Suchzeile oberhalb der Liste können Sie nach Namen nach Schwachstellen suchen.

- In Datei exportieren

  Durch Klicken auf die Schaltfläche **In Datei exportieren** können Sie die Schwachstellenliste in einer Datei speichern. Standardmäßig exportiert das Programm die Schwachstellenliste in eine CSV-Datei.

- Nur Schwachstellen anzeigen, die geschlossen werden können

Ist diese Option aktiviert, werden im Abschnitt Schwachstellen angezeigt, die durch einen Patch geschlossen werden können.

Ist diese Option deaktiviert, werden im Abschnitt Schwachstellen angezeigt, die durch einen Patch geschlossen werden können, sowie Schwachstellen, für die kein Patch vorhanden ist.

Diese Option ist standardmäßig aktiviert.

- **Eigenschaften**

  Wählen Sie in der Liste eine Software-Schwachstelle aus und klicken Sie auf **Eigenschaften**, um die Eigenschaften der ausgewählten Software-Schwachstelle in einem separaten Fenster anzuzeigen. In dem Fenster können Sie Folgendes tun:

  - Schwachstellen in Programmen auf diesem verwalteten Gerät ignorieren (in der Verwaltungskonsole oder in Kaspersky Security Center Cloud Console).
  - Liste mit Korrekturen anzeigen, die für die Schwachstelle empfohlen werden.
  - Software-Updates manuell angeben, um eine Schwachstelle zu beheben (in der Verwaltungskonsole oder in Kaspersky Security Center Cloud Console).
  - Schwachstellen-Instanzen anzeigen.
  - Liste der vorhandenen Aufgaben zur Schwachstellen-Behebung anzeigen, und neue Aufgaben zur Schwachstellen-Behebung erstellen.

Geräteauswahlen

Geräteauswahlen sind ein Instrument zum Filtern von Geräten nach festgelegten Bedingungen. Sie können Geräteauswahlen verwenden, um mehrere Geräte zu verwalten: beispielsweise, um einen Bericht über nur diese Geräte anzuzeigen, oder um alle diese Geräte in eine andere Gruppe zu verschieben.

Kaspersky Security Center Cloud Console bietet eine große Zahl an *vordefinierten Auswahlen* an (z. B. **Geräte mit dem Status "Kritisch"**, **Der Schutz ist deaktiviert**, **Aktive Bedrohungen werden erkannt**). Vordefinierte Auswahlen können nicht gelöscht werden. Sie können auch zusätzliche *benutzerdefinierte Auswahlen* definieren und anpassen.

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 Security Center Cloud Console können Sie die Liste mit Geräten einer Geräteauswahl anzeigen.

So zeigen Sie die Geräteliste aus der Geräteauswahl an:

1. Wechseln Sie im Hauptmenü zum Abschnitt **Geräte** → **Geräteauswahlen** oder **Gerätesuche und Softwareverteilung** → **Geräteauswahlen**.

2. Klicken Sie in der Auswahlliste auf den Namen der entsprechenden Geräteauswahl.

   Die Seite zeigt eine Tabelle mit Informationen zu den in der Geräteauswahl enthaltenen Geräten an.

3. Sie können die Daten der Gerätetabelle wie folgt gruppieren und filtern:

   - Klicken Sie auf das Einstellungen-Symbol ( ) und wählen Sie anschließend die Spalten aus, die in der Tabelle angezeigt werden sollen.

   - Klicken Sie auf das Filtersymbol ( ), geben Sie anschließend das Filterkriterium im aufgerufenen Menü 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 Zieladministrationsgruppe aus.

Geräteauswahl erstellen

Um eine Geräteauswahl zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Geräteauswahlen**.

   Eine Seite mit einer Liste von Geräteauswahlen wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Einstellungen der Geräteauswahl** wird geöffnet.

3. Geben Sie den Namen der neuen Auswahl ein.

4. Geben Sie die Gruppe an, in der die Geräte enthalten sind, die in die Geräteauswahl einbezogen werden sollen:

   - **Alle Geräte suchen** – Suche nach Geräten, die den Auswahlkriterien entsprechen und in den Gruppen **Verwaltete Geräte** oder **Nicht zugeordnete Geräte** enthalten sind.

   - **Verwaltete Geräte suchen** – Suche nach Geräten, die den Auswahlkriterien entsprechen und in den Gruppen **Verwaltete Geräte** enthalten sind.

   - **Nicht zugeordnete Geräte suchen** – Suche nach Geräten, die den Auswahlkriterien entsprechen und in den Gruppen **Nicht zugeordnete Geräte** enthalten sind.

   Sie können das Kontrollkästchen **Daten von sekundären Administrationsservern miteinbeziehen** aktivieren, um die Suche für Geräte zu aktivieren, die den Auswahlkriterien entsprechen 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 **Geräte** → **Geräteauswahlen**.

   Eine Seite mit einer Liste von Geräteauswahlen wird angezeigt.

2. Wählen Sie die relevante benutzerdefinierte Geräteauswahl aus und klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Fenster **Einstellungen der Geräteauswahl** wird geöffnet.

3. Klicken Sie auf der Registerkarte **Allgemein** auf den Link **Neue Bedingung**.

4. Geben Sie Bedingungen an, die erfüllt sein müssen, damit Geräte in die Auswahl aufgenommen werden.

5. Klicken Sie auf die Schaltfläche **Speichern**.

Die Einstellungen werden übernommen und gespeichert.

Nachfolgende werden die Einstellungen für Bedingungen der Aufnahme von Geräten in die Auswahl beschrieben. Die Bedingungen beruhen auf dem logischen ODER: In die Auswahl werden nur Geräte aufgenommen, die mindestens eine Bedingung erfüllen.

Allgemein

Im Abschnitt **Allgemein** kann der Name der Auswahlbedingung geändert sowie bestimmt werden, ob diese Auswahlbedingung umgekehrt werden soll:

Auswahlbedingung umkehren

Ist die Option aktiviert, so wird die vorgegebene Auswahlbedingung umgekehrt. Alle Geräte, die diese Bedingung nicht erfüllen, werden in die Auswahl aufgenommen.

Diese Option ist standardmäßig deaktiviert.

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.

- **Windows-Domäne**

  Es werden Geräte angezeigt, die zur angegebenen Windows-Domäne gehören.

- **Administrationsgruppe**

  Es werden Geräte angezeigt, die zur angegebenen Administrationsgruppe gehören.

- **Beschreibung**

Text, der im Eigenschaftenfenster des Geräts enthalten ist: im Feld **Beschreibung** des Abschnitts **Allgemein**.

Für die Beschreibung eines Textes im Feld **Beschreibung** sind die folgenden Zeichen zulässig:

- Innerhalb eines Wortes:
  - *****. Dieses Zeichen ersetzt beliebige Ausdrücke mit einer beliebigen Zahl von Zeichen.

  Beispiel:

  Für die Beschreibung der Wörter **Server** und **Server-**können Sie die Zeichenfolge **Server*** verwenden.

  - **?.** Dieses Zeichen ersetzt ein beliebiges Symbol.

  Beispiel:

  Für die Beschreibung der Wörter **Regel** oder **Regeln** können Sie die Zeichenfolge **Regel?** verwenden.

  Das Zeichen ***** oder **?** kann nicht als das erste Zeichen in einer Textbeschreibung verwendet werden.

- Zur Verknüpfung mehrerer Wörter:
  - Leerzeichen: Es werden alle Geräte angezeigt, deren Beschreibung ein beliebiges der angegebenen Wörter enthält.

  Beispiel:

  Zur Beschreibung einer Phrase, die entweder das Wort **Sekundär** oder **Virtuell** enthält, können Sie die Zeichenfolge **Sekundär Virtuell** verwenden.

  - **+**: Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort unbedingt im Text vorhanden sein muss.

  Beispiel:

  Zur Beschreibung einer Phrase, welche die beiden Wörter **Sekundär** und **Virtuell** enthält, können Sie den Ausdruck **+Sekundär+Virtuell** verwenden.

  - **-**: Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort im Suchtext nicht vorkommen darf.

  Beispiel:

  Zur Beschreibung einer Phrase, die das Wort **Sekundär** enthält, jedoch das Wort **Virtuell** nicht enthalten darf, können Sie den Ausdruck **+Sekundär-Virtuell** verwenden.

  - **"<Textabschnitt>"**: Ein in Anführungszeichen eingeschlossener Textabschnitt muss vollständig im Text vorhanden sein.

  Beispiel:

  Zur Beschreibung einer Phrase, welche die Wortverbindung **Sekundärer Server** enthält, können Sie den Ausdruck **"Sekundärer Server"** verwenden.

- IP-Bereich

Wenn diese Option aktiviert ist, können Sie in den Eingabefeldern die erste und die letzte IP-Adresse des Bereichs eingeben, zu dem die betreffenden Geräte gehören sollen.

Diese Option ist standardmäßig deaktiviert.

- Von einem anderen Administrationsserver verwaltet

  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 dem Active Directory-Verzeichnis 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 ist Mitglied in 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.

- Wechsel des Verbindungsprofils

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**. Das Programm 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 des verwalteten Programms anpassen:

- Gerätestatus

  In dieser Dropdown-Liste können Sie einen Gerätestatus auswählen: *OK*, *Kritisch* oder *Warnung*.

- **Status des Echtzeitschutzes**

  In dieser Dropdown-Liste können Sie den Wert für den Status des Echtzeitschutzes auswählen. Geräte mit dem angegebenen Echtzeitschutz-Status werden in die Auswahl aufgenommen.

- **Beschreibung des Gerätestatus**

  In diesem Feld können Sie die Kontrollkästchen für jene Bedingungen aktivieren, auf deren Basis einem Gerät eine der folgenden Statusvarianten zugewiesen werden soll: *OK, Kritisch* oder *Warnung*.

Im Unterabschnitt **Status der Komponenten der verwalteten Programme** können Sie Kriterien für die Aufnahme von Geräten in eine Auswahl anhand der Status der Komponenten der verwalteten Programme anpassen:

- **Status des Schutzes vor Datenverlust**

  Suche nach Geräten anhand des Status des "Schutzes vor Datenverlust" (*Keine Gerätedaten, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

- **Schutzstatus der Server für die Zusammenarbeit**

  Suche nach Geräten anhand des Status der Komponente "Schutz der Serverzusammenarbeit" (*Keine Gerätedaten*, *Beendet*, *Wird gestartet, Angehalten*, *Wird ausgeführt*, *Fehlgeschlagen*).

- **Antiviren-Schutzstatus der Mail-Server**

  Suche nach Geräten anhand des Status des Mail-Server-Schutzes (*Keine Gerätedaten, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

- **Status der Komponente "Endpoint Sensor"**

  Suche nach Geräten anhand des Status der Komponente "Endpoint Sensor" (*Keine Gerätedaten, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

Im Unterabschnitt **Statusbeeinflussende Probleme in verwalteten Programmen** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Liste von möglichen von einem verwalteten Programm gefundenen Problemen anpassen. Wenn zumindest ein ausgewähltes Problem auf einem Gerät existiert, wird das Gerät in die Auswahl aufgenommen. Wenn Sie ein Problem auswählen, das für mehrere Programme aufgelistet ist, haben Sie die Möglichkeit, dieses Problem in allen Listen automatisch auszuwählen.

Sie können die Kontrollkästchen für die Beschreibung der Status der verwalteten Programme aktivieren, bei deren Empfang die Geräte in die Auswahl aufgenommen werden. Wenn Sie einen Status auswählen, der für mehrere Programme aufgelistet ist, haben Sie die Möglichkeit, diesen Status in allen Listen automatisch auszuwählen.

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 Version des Updatepakets für das Betriebssystem angeben (im Format *X.Y*), das vorhanden sein muss, damit auf dem Gerät die Regel für das Verschieben angewandt wird. Standardmäßig ist keine Version angegeben.

- **Bitzahl des Betriebssystems**

  In dieser Dropdown-Liste können Sie die Architektur des Betriebssystems auswählen, die vorhanden sein muss, damit auf dem Gerät die Regel für das Verschieben angewandt wird (**Unbekannt**, **x86**, **AMD64**, **IA64**). Standardmäßig ist in dieser Liste keine Variante ausgewählt, die Architektur des Betriebssystems ist nicht angegeben.

- **Build-Version des Betriebssystems**

  Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

  Versionsnummer des Betriebssystems. Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Versionsnummer haben muss. Sie können auch eine Suche nach allen Versionsnummern mit Ausnahme der angegebenen anpassen.

- **Releasenummer des Betriebssystems**

  Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

  Release-Identifikator (ID) des Betriebssystems Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Release-ID haben muss. Sie können auch eine Suche nach allen Release-ID-Nummern mit Ausnahme der angegebenen anpassen.

Auf der Registerkarte **Virtuelle Maschinen** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anpassen, je nachdem, ob diese Geräte virtuelle Maschinen sind oder zur Virtual Desktop Infrastructure (VDI) gehören:

- **Ist eine virtuelle Maschine**

  Sie können in der Dropdown-Liste folgende Elemente wählen:

  - **Nicht definiert**.
  - **Nein**. Die gesuchten Geräte dürfen keine virtuellen Maschinen sein.
  - **Ja**. Die gesuchten Geräte müssen virtuelle Maschinen sein.

- Typ der virtuellen Maschine

  In der Dropdown-Liste können Sie den Hersteller der virtuellen Maschine auswählen.

  Die Dropdown-Liste ist verfügbar, wenn die Werte **Ja** oder **Unwichtig** in der Dropdown-Liste **Dies ist eine virtuelle Maschine** gewählt wurden.

- Teil einer Virtual Desktop Infrastructure (VDI)

  Sie können in der Dropdown-Liste folgende Elemente wählen:

  - **Nicht definiert**.
  - **Nein**. Die gesuchten Geräte dürfen kein Teil der Virtual Desktop Infrastructure (VDI) sein.
  - **Ja**. Die gesuchten Geräte müssen Teil der Virtual Desktop Infrastructure (VDI) sein.

Im Unterabschnitt **Hardware-Register** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der auf ihnen installierten Hardware anpassen:

Stellen Sie sicher, dass auf den Linux-Geräten, von denen Sie die Hardware-Details abrufen möchten, das Tool lshw installiert ist. Die von virtuellen Maschinen abgerufene Hardware-Details 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, die der in den Eingabefeldern angegebenen Taktrate entspricht (inklusive), werden in die Auswahl aufgenommen.

- **CPU-Taktrate MHz, bis**

  Die maximale Taktrate einer CPU. Geräte mit einer CPU, die der in den Eingabefeldern angegebenen Taktrate entspricht (inklusive), werden in die Auswahl aufgenommen.

- **Anzahl virtueller CPU-Kerne, von**

  Die minimale Anzahl virtueller CPU-Kerne. Geräte mit einer CPU, die dem in den Eingabefeldern angegebenen Bereich der virtuellen Kerne entspricht (inklusive), werden in die Auswahl aufgenommen.

- **Anzahl virtueller CPU-Kerne, bis**

  Die maximale Anzahl virtueller CPU-Kerne. Geräte mit einer CPU, die dem in den Eingabefeldern angegebenen Bereich der virtuellen Kerne entspricht (inklusive), werden in die Auswahl aufgenommen.

- **Größe der Festplatte (GB), von**

  Die minimale Größe der Festplatte des Geräts. Geräte mit Festplatten, die dem in den Eingabefeldern angegebenen Bereich entsprechen (inklusive), werden in die Auswahl aufgenommen.

- Größe der Festplatte (GB), bis

  Die maximale Größe der Festplatte des Geräts. Geräte mit Festplatten, die dem in den Eingabefeldern angegebenen Bereich entsprechen (inklusive), werden in die Auswahl aufgenommen.

- RAM-Größe in MB, von

  Die minimale Größe des Arbeitsspeichers des Geräts. Geräte mit Arbeitsspeicher, der dem Größenbereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

- Speichergröße MB, bis

  Die maximale 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 Programmen anpassen:

- Programmname

  In dieser Dropdown-Liste können Sie ein Programm auswählen. Die Geräte, auf denen dieses Programm installiert ist, werden in die Auswahl aufgenommen.

- Programmversion

  Geben Sie in diesem Eingabefeld die Version des ausgewählten Programms ein.

- Hersteller

  In dieser Dropdown-Liste können Sie den Hersteller des auf dem Gerät installierten Programms auswählen.

- Programmstatus

  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.

- Nach Update suchen

  Wenn diese Option aktiviert ist, erfolgt die Suche anhand der Updatedaten der auf den Geräten installierten Programme. Nachdem Sie das Kontrollkästchen aktiviert haben, ändern sich die Felder **Programmname**, **Programmversion** und **Programm-Status** in **Update-Name**, **Update-Version** und **Status**.

  Diese Option ist standardmäßig deaktiviert.

- Name der inkompatiblen Sicherheitsanwendung

In dieser Dropdown-Liste können Sie Sicherheitsanwendungen von Drittherstellern auswählen. Bei der Suche werden Geräte in die Auswahl aufgenommen, auf denen das ausgewählte Programm installiert wurde.

- Programm-Tag

  In dieser Dropdown-Liste können Sie einen Programm-Tag auswählen. Alle Geräte, auf denen Programme installiert sind, die den ausgewählten Tag in der Beschreibung haben, werden in die Geräteauswahl aufgenommen.

- Auf Geräte ohne angegebene Tags anwenden

  Wenn diese Option aktiviert ist, werden Geräte, in deren Beschreibung keines der gewählten Tags vorkommt, in die Auswahl aufgenommen.

  Wenn diese Option deaktiviert ist, wird das Kriterium nicht angewendet.

  Diese Option ist standardmäßig deaktiviert.

Im Unterabschnitt **Schwachstellen und Updates** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Quelle der Windows-Updates anpassen:

WUA wurde auf den Administrationsserver umgeschaltet

In dieser Dropdown-Liste können Sie eine der folgenden Varianten der Suche auswählen:

- **Ja**. Bei Auswahl dieser Option werden Geräte in die Suchergebnisse aufgenommen, die Windows-Updates vom Administrationsserver herunterladen.
- **Nein**. Bei Auswahl dieser Option werden Geräte in die Ergebnisse aufgenommen, die Windows-Updates von einer anderen Quelle herunterladen.

Details zu Programmen von Kaspersky

Im Unterabschnitt **Programme von Kaspersky** können Sie die Kriterien für die Aufnahme von Geräten anhand des ausgewählten verwalteten Programms konfigurieren:

- Programmname

  In der Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl wählen, wenn die Suche anhand des Namens des Kaspersky-Programms erfolgt.

  In der Liste sind nur die Programme aufgeführt, für die Verwaltungs-Plug-ins im Administrator-Arbeitsplatz installiert sind.

  Wurde kein Programm gewählt, wird kein Kriterium angewandt.

- Programmversion

In diesem Eingabefeld können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl angeben, wenn die Suche nach Versionsnummer des Kaspersky-Programms 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 Programm-Module ausgeführt wurde.

  Ist das Kontrollkästchen deaktiviert, wird das Kriterium nicht angewandt.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Gerät wird über Kaspersky Security Center 14.2 verwaltet**

  Mithilfe dieser Dropdown-Liste können Geräte in die Auswahl aufgenommen werden, die über Kaspersky Security Center Cloud Console verwaltet werden:

  - **Ja**. Geräte werden in die Auswahl aufgenommen, wenn sie über Kaspersky Security Center Cloud Console verwaltet werden.
  - **Nein**. Das Programm nimmt Geräte in die Auswahl auf, wenn sie nicht über Kaspersky Security Center Cloud Console 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**. Das Programm 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 Security Center Cloud Console 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*, *Startet*, *Wird ausgeführt*, *Fehlgeschlagen*, *Nicht installiert*, *Von 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 wurde angehalten, z. B. nachdem der Benutzer den Schutz in der verwalteten Anwendung angehalten hat.
- *Startet* – 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 Lizenz nicht unterstützt* Die Lizenz deckt die ausgewählte Komponente nicht ab.

Im Gegensatz zu anderen Statuswerten wird der Status *Keine Daten* nicht vom Programmen gesendet. Diese Option zeigt, dass die Programme über keine Informationen über den ausgewählten Status der Komponente aufweisen. Dies kann beispielsweise der Fall sein, wenn die ausgewählte Komponente zu keiner der auf dem Gerät installierten Anwendungen gehört oder wenn das Gerät ausgeschaltet ist.

- **Version**

  Suche nach Geräten anhand der Versionsnummer der in der Liste ausgewählten Komponente. Sie können eine Versionsnummer eingeben, beispielsweise `3.4.1.0`, und dann festlegen, ob die ausgewählte Komponente eine gleich, frühere oder spätere Version aufweisen muss. Sie können auch eine Suche nach allen Versionen mit Ausnahme der angegebenen anpassen.

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 Tags aus, indem Sie auf das Eingabefeld **Tag** klicken. Geben Sie an, ob die Geräte mit den ausgewählten Tags in die Geräteauswahl aufgenommen oder von ihre ausgeschlossen werden sollen.

- **Muss vorhanden sein**

  Wenn diese Variante ausgewählt ist, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibung der ausgewählte Tag vorhanden ist. Bei der Gerätesuche können Sie das Zeichen * verwenden, um eine beliebige Zeile mit einer beliebigen Anzahl von Zeichen zu ersetzen.

  Diese Variante ist standardmäßig ausgewählt.

- **Darf nicht vorhanden sein**

  Wenn diese Variante ausgewählt ist, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibung der ausgewählte Tag nicht vorhanden ist. Bei der Gerätesuche können Sie das Zeichen * verwenden, um eine beliebige Zeile mit einer beliebigen Anzahl von Zeichen zu ersetzen.

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 der Kaspersky Security Center Cloud Console 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 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 **Zeilen 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. Wechseln Sie im Hauptmenü zu **Geräte** → **Geräteauswahlen** oder zu **Gerätesuche und Softwareverteilung** → **Geräteauswahlen**.
2. Klicken Sie in der Auswahlliste auf den Namen der entsprechenden Geräteauswahl.

   Die Seite zeigt eine Tabelle mit Informationen zu den in der Geräteauswahl enthaltenen Geräten an.
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.

Anzeigen und Anpassen der Aktionen, 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. Wechseln Sie im Hauptmenü zu **Geräte** → **Gruppenhierarchie**.
2. Klicken Sie auf den Namen der gewünschten Administrationsgruppe.

   Das Eigenschaftenfenster der übergeordneten Administrationsgruppe wird geöffnet.
3. Wechseln 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.

- Vererben der Einstellungen für untergeordnete Gruppen erzwingen

  Die Einstellungswerte werden an untergeordnete Gruppen verteilt, aber in den Eigenschaften der untergeordneten Gruppen sind diese Einstellungen gesperrt.

  Diese Option ist standardmäßig deaktiviert.

5. Aktivieren oder deaktivieren Sie im Abschnitt **Geräteaktivität** die folgenden Optionen:

   - Administrator benachrichtigen, wenn Gerät inaktiv seit mehr als (Tage)

     Wenn diese Option aktiviert ist, erhält der Administrator Benachrichtigungen über inaktive Geräte. Sie können das Zeitintervall angeben, nach dem das Ereignis **Gerät zu lange inaktiv im Netzwerk** erstellt wird. Standardmäßig beträgt das Zeitintervall 7 Tage.

     Diese Option ist standardmäßig aktiviert.

   - Gerät aus Gruppe entfernen, wenn Gerät inaktiv seit mehr als (Tage)

     Wenn diese Option aktiviert ist, können Sie das Zeitintervall festlegen, nach dem das Geräte automatisch aus der Gruppe gelöscht wird. Standardmäßig beträgt das Zeitintervall 60 Tage.

     Diese Option ist standardmäßig aktiviert.

6. Klicken Sie auf die Schaltfläche **Speichern**.

   Ihre Änderungen werden gespeichert und übernommen.

Über die Varianten für den Gerätestatus

Kaspersky Security Center Cloud Console 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 Security Center Cloud Console in bestimmten Fällen das Sichtbarkeits-Flag des Gerätes im Netzwerk (siehe folgende Tabelle). Wenn Kaspersky Security Center Cloud Console 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
Es wurde keine Sicherheitsanwendung installiert	Auf dem Gerät ist der Administrationsagent installiert, aber es wurde keine Sicherheitsanwendung installiert.	• Umschalter aktiviert. • Umschalter deaktiviert.
Zu viele Viren gefunden	Auf dem Gerät wurden 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 eine Sicherheitsanwendung wurde auf dem Gerät installiert, aber es wurden weder die Aufgabe zur *Schadsoftware-Untersuchung* noch eine lokale Untersuchungsaufgabe innerhalb des angegebenen Zeitintervalls ausgeführt. Die Bedingung gilt nur für Geräte, die vor mehr als sieben Tagen zur Datenbank des Administrationsservers 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 Datenbank des Administrationsservers hinzugefügt wurden.	Über 1 Tag.
Die letzte Verbindung liegt lange zurück	Der Administrationsagent ist auf dem Gerät installiert, es wurde allerdings nicht innerhalb des angegebenen Zeitintervalls mit dem Administrationsserver verbunden, da es deaktiviert ist.	Über 1 Tag.
Aktive Bedrohungen werden erkannt	Die Anzahl der unbearbeiteten Objekte im Ordner **Aktive Bedrohungen** übersteigt den angegebenen Wert.	Über 0 Elemente.
Neustart erforderlich	Das Gerät ist im Netzwerk sichtbar, aber ein Programm 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	Das Gerät ist im Netzwerk sichtbar, aber infolge der Inventarisierung der Software durch den	• Umschalter deaktiviert.

installiert	Administrationsagenten wurden auf dem Gerät inkompatible Programme gefunden.	• 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.	Über 0 Tage.
Die letzte Suche nach Windows-Updates liegt lange zurück	Das Gerät ist im Netzwerk sichtbar, aber die Aufgabe "Windows-Updates synchronisieren" 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	Die Einstellungen des mobilen Geräts unterscheiden sich von den in der Richtlinie von	• Umschalter deaktiviert.

entsprechen nicht der Richtlinie	Kaspersky Endpoint Security für Android festgelegten Einstellungen beim Ausführen der Untersuchung der Übereinstimmungsregeln.	• Umschalter aktiviert.
Es wurden unbearbeitete Vorfälle erkannt	Auf dem Gerät sind unbearbeitete Vorfälle vorhanden. Vorfälle können sowohl automatisch mithilfe von auf dem Client-Gerät installierten Verwaltungsprogrammen von Kaspersky als auch manuell durch den Administrator erstellt werden.	• Umschalter deaktiviert. • Umschalter aktiviert.
Gerätestatus wird vom Programm bestimmt	Der Gerätestatus wird vom verwalteten Programm bestimmt.	• Umschalter deaktiviert. • Umschalter 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.	Über 0 Minuten.
Die Sicherheitsanwendung wurde nicht gestartet	Das Gerät ist im Netzwerk sichtbar und eine Sicherheitsanwendung ist auf dem Gerät installiert, wurde aber nicht gestartet.	• Umschalter deaktiviert. • Umschalter aktiviert.

Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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*.

Einstellungen zum Umschalten der Status von Geräten

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 **Geräte** → **Gruppenhierarchie**.
2. Klicken Sie in der angezeigten Liste der Gruppen auf den Link mit dem Namen der Gruppe, für die Sie den Wechsel der Gerätestatus ändern möchten.
3. Klicken Sie im daraufhin geöffneten Eigenschaftenfenster auf die Registerkarte **Gerätestatus**.
4. Wählen Sie im linken Fensterbereich die Option **Kritisch** aus.
5. Aktivieren Sie im rechten Bereich im Abschnitt **Werte, für die der Status auf "Kritisch" gesetzt wird** die Bedingung zum Umschalten eines Geräts in den Status *Kritisch*.

   Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

6. Aktivieren Sie das Optionsfeld neben der Bedingung in der Liste.
7. Klicken Sie in der oberen linken Ecke der Liste auf die Schaltfläche **Bearbeiten**.
8. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.

   Es können nicht für alle Bedingungen Werte festgelegt werden.
9. Klicken Sie auf die Schaltfläche **OK**.

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Kritisch*.

Um die Änderungen des Gerätestatus auf Warnung zu aktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Gruppenhierarchie**.
2. Klicken Sie in der angezeigten Liste der Gruppen auf den Link mit dem Namen der Gruppe, für die Sie den Wechsel der Gerätestatus ändern möchten.
3. Klicken Sie im daraufhin geöffneten Eigenschaftenfenster auf die Registerkarte **Gerätestatus**.
4. Wählen Sie im linken Fensterbereich die Option **Warnung** aus.
5. Aktivieren Sie im rechten Bereich im Abschnitt **Werte, für die der Status auf "Warnung" gesetzt wird** die Bedingung zum Umschalten eines Geräts in den Status *Warnung*.

   Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

6. Aktivieren Sie das Optionsfeld neben der Bedingung in der Liste.
7. Klicken Sie in der oberen linken Ecke der Liste auf die Schaltfläche **Bearbeiten**.

8. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.

   Es können nicht für alle Bedingungen Werte festgelegt werden.

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

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Warnung*.

Administrationsserver für Client-Geräte wechseln

Sie können den Administrationsserver, der die Client-Geräte verwaltet, durch einen anderen Administrationsserver mit der Aufgabe **Administrationsserver wechseln** 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. Wechseln Sie im Hauptmenü zu **Geräte** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

3. Wählen Sie für Kaspersky Security Center Cloud Console den Aufgabentyp **Administrationsserver wechseln**.
4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen.

   Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.

5. Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll.
6. Wählen Sie den Administrationsserver aus, den Sie für die Verwaltung der ausgewählten Geräte verwenden möchten.
7. Legen Sie die Benutzerkonto-Einstellungen fest:

   - **Standardbenutzerkonto**

     Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, unter dem das Programm installiert und gestartet wurde, dass diese Aufgabe ausführt.

     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 dessen Namen 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 allgemeinen Aufgabeneinstellungen entsprechend Ihrer Bedürfnisse 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.

Über Cluster und Server-Arrays

Die Kaspersky Security Center Cloud Console unterstützt Cluster-Technologie. Sobald der Administrationsserver vom Administrationsagenten die Information erhält, dass ein auf einem Client-Gerät installiertes Programm zum Server-Array gehört, wird das betreffende Client-Gerät als Knoten in dem Cluster eingebunden.

Wenn eine Administrationsgruppe Cluster oder Server-Arrays enthält, zeigt die Seite **Verwaltete Geräte** zwei Registerkarten an – eine für einzelne Geräte und eine für Cluster und Server-Arrays. Nachdem die verwalteten Geräte als Cluster-Knoten erkannt wurden, wird der Cluster als einzelnes Objekt zur Registerkarte **Cluster und Server-Arrays** hinzugefügt.

Die Knoten des Clusters oder Server-Arrays werden zusammen mit anderen verwalteten Geräten auf der Registerkarte **Geräte** angezeigt. Sie können für die Knoten wie für andere Geräte Eigenschaften anzeigen und weitere Operationen durchführen, aber Sie können einen Cluster-Knoten nicht löschen oder ihn getrennt von seinem Cluster in eine andere Administrationsgruppe verschieben. Sie können nur einen ganzen Cluster löschen oder verschieben.

Die folgenden Vorgänge können Sie mit Clustern oder Server-Arrays ausführen:

- Eigenschaften anzeigen
- Das Cluster oder Server-Array in eine andere Administrationsgruppe verschieben

Wenn Sie ein Cluster oder Server-Array in eine andere Gruppe verschieben, werden alle ihre Knoten mit verschoben, da ein Cluster und alle seine Knoten immer derselben Administrationsgruppe angehören.

- Löschen

  Es ist nur dann sinnvoll, ein Cluster oder ein Server-Array zu löschen, wenn das Cluster oder Server-Array nicht mehr im Netzwerk der Organisation existiert. Wenn ein Cluster noch in Ihrem Netzwerk sichtbar ist und der Administrationsagent und die Kaspersky-Sicherheitsanwendung noch auf den Cluster-Knoten installiert sind, fügt Kaspersky Security Center Cloud Console 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. Wechseln Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte** → **Cluster und Server-Arrays**.

   Die Liste der Cluster und Server-Arrays wird angezeigt.

2. Klicken Sie auf den Namen des erforderlichen Clusters oder Server-Arrays.

Das Eigenschaftenfenster des gewählten Clusters oder Server-Arrays wird geöffnet.

Allgemein

Der Abschnitt **Allgemein** zeigt allgemeine Informationen zu dem Cluster oder Server-Array an. Die Informationen beruhen auf Daten, die bei der letzten Synchronisierung der Cluster-Knoten mit dem Administrationsserver empfangen wurden:

- **Name**
- **Beschreibung**
- **Windows-Domäne**

  Windows-Domäne oder -Arbeitsgruppe, die das Cluster oder Server-Array enthält.

- **NetBIOS-Name**

  Windows-Netzwerkname des Clusters oder Server-Arrays.

- **DNS-Name**

  Name der DNS-Domäne des Clusters oder Server-Arrays.

Aufgaben

In der Registerkarte **Aufgaben** können Sie die dem Cluster oder Server-Array zugewiesenen Aufgaben verwalten: Liste der vorhandenen Aufgaben anzeigen, neue Aufgaben erstellen, Aufgaben entfernen, starten und beenden, Aufgabeneinstellungen ändern und die Ergebnisse der Aufgabenausführung anzeigen. Die aufgeführten Aufgaben beziehen sich auf die Kaspersky-Sicherheitsanwendung, die auf den Cluster-Knoten installiert ist.
Kaspersky Security Center Cloud Console 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-Programm

Das Eigenschaftenfenster kann auch zusätzliche Registerkarten mit Informationen und Einstellungen bezüglich der auf den Cluster-Knoten installierten Kaspersky-Sicherheitsanwendung enthalten.

Geräte-Tags

Dieser Abschnitt beschreibt Geräte-Tags und enthält eine Anleitung für deren Erstellung und Änderung sowie für die manuelle bzw. automatische Zuweisung von Tags an Geräte.

Über Geräte-Tags

Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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. 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. Wechseln Sie im Hauptmenü zu **Geräte** → **Tags** → **Tags des Geräts**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
   Ein neues Tag-Fenster öffnet sich.
3. Geben Sie im Feld **Tag** den Namen des Tags ein.
4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Das neue Tag wird in der Liste der Geräte-Tags angezeigt.

Geräte-Tag umbenennen

Um ein Geräte-Tag umzubenennen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Tags** → **Tags des Geräts**.
2. Klicken Sie auf den Namen des Tags, das Sie umbenennen möchten.
   Ein Fenster mit den Tag-Eigenschaften wird geöffnet.
3. Ändern Sie im Feld **Tag** den Tag-Namen.
4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Das aktualisierte Tag wird in der Liste der Geräte-Tags angezeigt.

Geräte-Tag löschen

Um ein Geräte-Tag zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Tags** → **Tags des Geräts**.
2. Wählen Sie in der Liste das Geräte-Tag aus, das Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie im folgenden Fenster auf **Ja**.

Das Geräte-Tag wird gelöscht. Das gelöschte Tag wird automatisch von allen Geräten entfernt, denen es zugewiesen war.

Das von Ihnen gelöschte Tag wird nicht automatisch aus den Regeln für die automatische Tag-Zuweisung entfernt. Nach dem Löschen des Tags wird es nur dann einem neuen Gerät zugewiesen, wenn das Gerät die Bedingungen der Regel erfüllt, die das Tag zuweist.

Das gelöschte Tag wird nicht automatisch vom Gerät entfernt, wenn dieses Tag dem Gerät von einem Programm oder einem Administrationsagenten zugewiesen wurde. Um das Tag von Ihrem Gerät zu entfernen, verwenden Sie das Tool "klscflag".

Anzeigen von Geräten, denen ein Tag zugewiesen ist

So zeigen Sie Geräte an, denen ein Tag zugewiesen ist:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Tags** → **Tags des Geräts**.
2. Klicken Sie auf den Link **Geräte anzeigen** neben dem Tag, für das Sie zugewiesene Geräte anzeigen möchten.
   Wenn Sie nicht den Link **Geräte anzeigen** neben einem Tag sehen, wird das Tag keinem Gerät zugewiesen.

Die Liste der angezeigten Geräte zeigt nur die Geräte an, denen das Tag zugewiesen ist.

Klicken Sie auf Ihrem Browser auf die Schaltfläche **Zurück**, um zur Liste der Geräte-Tags zurückzukehren.

Anzeigen von Tags, die einem Gerät zugewiesen sind

So zeigen Sie einem Gerät zugewiesene Tags an:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte**.
2. Klicken Sie auf den Namen des Geräts, dessen Tags Sie anzeigen möchten.
3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts die Registerkarte **Tags** aus.

Die Liste der dem ausgewählten Gerät zugewiesenen Tags wird angezeigt.

Sie können dem Gerät ein anderes Tag zuweisen oder ein bereits zugewiesenes Tag entfernen. Darüber hinaus können Sie alle Geräte-Tags ansehen, die auf dem Administrationsserver vorhanden sind.

Manuelle Zuweisung von Tags an ein Gerät

So weisen Sie einem Gerät ein Tag manuell zu:

1. Zeigen Sie dem Gerät zugeordnete Tags an, dem Sie einen anderen Tag zuweisen möchten.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Führen Sie im folgenden Fenster einen der folgenden Schritte aus:

- Um ein neues Tag zu erstellen und zuzuweisen, wählen Sie **Neues Tag erstellen** und geben Sie den Namen des neuen Tags ein.
- Um ein vorhandenes Tag auszuwählen, wählen Sie **Vorhandenes Tag zuordnen** und dann in der Dropdown-Liste das gewünschte Tag.

4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu übernehmen.
5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Das ausgewählte Tag wird dem Gerät zugewiesen.

Entfernen eines zugewiesenen Tags von einem Gerät

So entfernen Sie ein Tag von einem Gerät:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte**.
2. Klicken Sie auf den Namen des Geräts, dessen Tags Sie anzeigen möchten.
3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts die Registerkarte **Tags** aus.
4. Aktivieren Sie das Kontrollkästchen neben dem Tag, das Sie entfernen möchten.
5. Klicken Sie am oberen Ende der Liste auf die Schaltfläche **Tag-Zuweisen aufheben**.
6. Klicken Sie im folgenden Fenster auf **Ja**.

Das Tag wurde vom Gerät entfernt.

Das nicht zugewiesene Geräte-Tag wird nicht gelöscht. Bei Bedarf können Sie es manuell löschen.

Sie können Tags, die dem Gerät von Programmen oder Administrationsagenten zugewiesen wurden, nicht manuell entfernen. Verwenden Sie zum entfernen dieser Tags das Tool "klscflag".

Regeln für das automatische Zuweisen von Tags an Geräten anzeigen

So zeigen Sie Regeln für die automatischer Zuweisung von Tags an Geräte an:

Führen Sie eine beliebige der folgenden Aktionen aus:

- Wechseln Sie im Hauptmenü zu **Geräte** → **Tags** → **Regeln für die automatische Tag-Zuweisung**.
- Wechseln Sie im Hauptmenü zu **Geräte** → **Tags** → **Tags des Geräts** und klicken Sie anschließend auf den Link **Regeln für die automatische Tag-Zuweisung einrichten**.
- Zeigen Sie die Tags an, die einem Gerät zugeordnet sind, und klicken Sie dann auf **Einstellungen**.

Die Liste der Regeln für die automatische Tag-Zuweisung von Geräten wird angezeigt.

Regeln für das automatische Zuweisen von Tags an Geräte bearbeiten

So bearbeiten Sie die Regeln für das automatische Zuweisen von Tags an Geräte:

1. Zeigen Sie die Regeln für das automatische Zuweisen von Tags an Geräte an.
2. Klicken Sie auf den Namen der Regel, die Sie bearbeiten möchten.
   Es wird ein Fenster zum Erstellen neuer Regeln geöffnet.
3. Bearbeiten Sie die allgemeinen Eigenschaften der Regel:
   a. Ändern Sie im Feld **Regelname** den Regelnamen.
      Der Name darf nicht mehr als 256 Zeichen umfassen.
   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 umfassen.

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 umfassen.

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 umfassen. Der Name darf sich innerhalb einer Regel nicht wiederholen.

6. Passen Sie das Auslösen der Regel entsprechend den folgenden Bedingungen an: Es können mehrere Bedingungen ausgewählt werden.

- **Netzwerk** – Netzwerkeigenschaften des Gerätes (beispielsweise Gerätename im Windows-Netzwerk oder Zugehörigkeit des Gerätes zu einer Domäne oder einem IP-Subnetz).

  Wenn für die Datenbank, die Sie für Kaspersky Security Center Cloud Console 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.

- **Programme** – Vorhandensein des Administrationsagenten auf dem Gerät, Typ, Version und Betriebssystemarchitektur.
- **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.

Quarantäne und Backup

Auf den Client-Geräten installierte Antiviren-Programme von Kaspersky können während der Untersuchung von Geräten die Dateien in Quarantäne oder ins Backup verschieben.

Die *Quarantäne* ist ein spezieller Speicher, in den Dateien verschoben werden, die möglicherweise von Viren infiziert oder im Augenblick des Fundes irreparabel sind.

Das *Backup* dient zur Speicherung der Backup-Kopien von Dateien, die gelöscht oder bei der Desinfizierung verändert wurden.

Kaspersky Security Center Cloud Console erstellt eine gemeinsame Liste von Dateien, die von Kaspersky-Programmen auf den Client-Geräten in die Quarantäne oder ins Backup verschoben werden. Die Administrationsagenten der Client-Geräte leiten Informationen über die Dateien in der Quarantäne und im Backup an den Administrationsserver weiter.

Kaspersky Security Center Cloud Console 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 Security Center Cloud Console ermöglicht es, Kopien von Dateien herunterzuladen, die von einer Sicherheitsanwendung in die Quarantäne oder ins Backup 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.

Um eine Kopie der Datei aus der Quarantäne oder dem Backup auf eine Festplatte zu speichern, gehen Sie wie folgt vor:

1. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie eine Kopie der Datei aus der Quarantäne speichern wollen, wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Quarantäne**.

   - Wenn Sie eine Kopie der Datei aus dem Backup speichern möchten, wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Backup**.

2. Wählen Sie in dem sich öffnenden Fenster eine Datei aus, die Sie herunterladen möchten und klicken Sie auf **Herunterladen**.

   Der Download wird gestartet. Eine Kopie der Datei, die sich in der Quarantäne des Client-Geräts befindet, wird im angegebenen Order gespeichert.

Dateien aus der Datenverwaltung entfernen

Um eine Datei in Quarantäne oder im Backup zu löschen, gehen Sie wie folgt vor:

1. Führen Sie eine der folgenden Aktionen aus:

- Wenn Sie eine Kopie der Datei aus der Quarantäne speichern wollen, wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Quarantäne**.

- Wenn Sie eine Kopie der Datei aus dem Backup speichern möchten, wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Backup**.

2. Wählen Sie in dem sich öffnenden Fenster eine Datei aus, die Sie löschen möchten und klicken Sie auf **Löschen**.

3. Bestätigen Sie, dass Sie die Datei löschen möchten.

Die Sicherheitsanwendung auf dem Client-Gerät mit platzierten Dateien in der Datenverwaltung (Quarantäne oder Backup) löscht die gleichen Dateien aus der Datenverwaltung.

Ferndiagnose der Client-Geräte

Sie können die Ferndiagnose für das Remote-Ausführen der folgenden Vorgänge auf Windows-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-basierten Client-Geräten durchzuführen, müssen Sie zunächst das Fenster für die Ferndiagnose öffnen.

So öffnen Sie das Fenster für die Ferndiagnose:

1. Führen Sie einen der folgenden Schritte aus, um das Gerät auszuwählen, für welches Sie das Ferndiagnosefenster öffnen möchten:

   - Wenn das Gerät zu einer Administrationsgruppe gehört, wechseln Sie im Hauptmenü zu **Geräte → Gruppen → <Gruppenname> → Verwaltete Geräte**.

   - Wenn das Gerät zur Gruppe nicht zugeordneter Geräte gehört, wechseln Sie im Hauptmenü zu **Gerätesuche und Softwareverteilung → Nicht zugeordnete Geräte**.

2. Klicken Sie auf den Namen des gewünschten Geräts.

3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts die Registerkarte **Erweitert** aus.

4. Klicken Sie im folgenden Fenster auf **Remote-Diagnose**.

   Dies öffnet das Fenster **Remote-Diagnose** eines Client-Geräts. Wenn zwischen dem Administrationsserver und dem Client-Gerät keine Verbindung hergestellt werden kann, wird eine Fehlermeldung angezeigt.

Aktivieren und Deaktivieren der Ablaufverfolgung für Programme

Sie können die Ablaufverfolgung, einschließlich Xperf-Ablaufverfolgung, aktivieren und deaktivieren.

Ablaufverfolgung aktivieren und deaktivieren

Um die Ablaufverfolgung auf einem Remote-Gerät zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.

2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Programme von Kaspersky** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Programme 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.

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 **Programme von Kaspersky** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Programme angezeigt.

3. Wählen Sie in der Liste der Programme das Programm "Kaspersky Endpoint Security für Windows" aus.

   Die Liste mit Optionen zur Ferndiagnose für Kaspersky Endpoint Security für Windows wird angezeigt.

4. Klicken Sie im Abschnitt **Xperf-Ablaufverfolgung** auf **Xperf-Ablaufverfolgung aktivieren**.

   Wenn die Xperf-Ablaufverfolgung bereits aktiviert ist, wird stattdessen die Schaltfläche **Xperf-Ablaufverfolgung deaktivieren** angezeigt. Klicken Sie auf diese Schaltfläche, wenn Sie die Xperf-Ablaufverfolgung für Kaspersky Endpoint Security für Windows deaktivieren möchten.

5. Wählen Sie im nächsten Fenster **Xperf-Ablaufverfolgungsstufe ändern** eine der folgenden Ablaufverfolgungsstufen entsprechend den Anweisungen des Spezialisten des technischen Supports aus:

   a. Wählen Sie eine der folgenden Ablaufverfolgungsstufen aus:

   - **Leichte Stufe**

     Eine Protokolldatei dieses Typs enthält die Mindestmenge an Informationen über das System.

     Diese Variante ist standardmäßig ausgewählt.

   - **Tiefe Stufe**

     Eine Protokolldatei dieses Typs enthält detailliertere Informationen als Protokolldateien vom Typ *Leicht* und kann von den Experten des Technischen Supports angefordert werden, wenn eine Protokolldatei vom Typ *Leicht* nicht für die Beurteilung der Leistung ausreicht. Die Protokolldatei der Stufe *Tief* enthält technische Informationen zum System einschließlich: Informationen zur Hardware und zum Betriebssystem; Liste der gestarteten und abgeschlossenen Prozesse und Anwendungen; Ereignisse, die für die Leistungsbewertung verwendet wurden; Ereignisse aus dem Windows-Systembewertungstool.

   b. Wählen Sie eine der folgenden Xperf-Ablaufverfolgungstypen aus:

   - **Basistyp**

Die Ablaufverfolgungsinformationen werden während der Ausführung der Sicherheitsanwendung Kaspersky Endpoint Security empfangen.

Diese Variante ist standardmäßig ausgewählt.

- **Bei-Neustart-Typ**

  Die Ablaufverfolgungsinformationen werden empfangen, während das Betriebssystem auf dem verwalteten Gerät gestartet wird. Diese Art von Ablaufverfolgung ist wirksam, wenn das Problem, das die Systemleistung beeinträchtigt, nach dem Einschalten des Geräts und vor dem Start von Kaspersky Endpoint Security auftritt.

Sie werden möglicherweise auch aufgefordert, die Option **Größe der Dateien in Rotation, in MB** zu aktivieren, um eine übermäßige Größenzunahme der Protokolldateien zu vermeiden. Geben Sie dann die maximale Größe der Protokolldatei an. Wenn die Datei die maximale Größe erreicht, werden die ältesten Informationen der Ablaufverfolgung durch neue Informationen überschrieben.

c. Legen Sie die Größe der Rotationsdatei fest.

d. Klicken Sie auf die Schaltfläche **Speichern**.

Die Xperf-Ablaufverfolgung ist aktiviert und konfiguriert.

6. Wenn Sie die Xperf-Ablaufverfolgung für Kaspersky Endpoint Security für Windows deaktivieren möchten, klicken Sie im Abschnitt **Xperf-Ablaufverfolgung** auf **Xperf-Ablaufverfolgung deaktivieren**.

   Die Xperf-Ablaufverfolgung ist deaktiviert.

Herunterladen der Protokolldateien eines Programms

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 **Programme von Kaspersky** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Programme angezeigt.

3. Wählen Sie in der Liste der Programme jenes aus, für das Sie die Protokolldatei herunterladen möchten.

4. Klicken Sie im Abschnitt **Ablaufverfolgung** auf **Protokolldateien**.

   Dadurch wird das Fenster **Ablaufverfolgungsprotokolle des Geräts** geöffnet, welches eine Liste von Protokolldateien anzeigt.

5. Wählen Sie in der Liste der Protokolldateien die Datei aus, die Sie herunterladen möchten.

6. Führen Sie eine der folgenden Aktionen aus:

   - Laden Sie die ausgewählte Datei durch klicken auf **Herunterladen** herunter. Sie können mehrere Dateien zum Herunterladen auswählen.

   - Um einen Teil der ausgewählten Datei herunterzuladen:

     a. Klicken Sie auf die Schaltfläche **Einen Teil herunterladen**.

     Das gleichzeitige Herunterladen von Teilen mehrerer Dateien ist nicht möglich. Wenn Sie mehr als eine Protokolldatei auswählen, wird die Schaltfläche **Einen Teil herunterladen** deaktiviert.

     b. Geben Sie im folgenden Fenster den Namen und den herunterzuladenden Teil der Datei entsprechend Ihren Anforderungen an.

     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 **Programme von Kaspersky** aus.
3. Klicken Sie im Abschnitt **Programmeinstellungen** auf die Schaltfläche **Herunterladen**, um Informationen über die Einstellungen der auf dem Client-Gerät installierten Anwendungen herunterzuladen.

Das zip-Archiv mit Informationen wird an den angegebenen Speicherort heruntergeladen.

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 Protokolle des Geräts**.
3. Wählen Sie im Fenster **Alle Protokolle des Geräts** die erforderlichen Protokolle aus.
4. Führen Sie eine der folgenden Aktionen aus:
   - Laden Sie das ausgewählte Protokoll durch klicken auf **Vollständige Datei herunterladen** herunter.

- 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 **Programme von Kaspersky** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Programme angezeigt.
3. Wählen Sie in der Liste der Programme das Programm aus, dass Sie starten, stoppen oder neu starten möchten.
4. Wählen Sie eine Aktion aus, indem Sie auf eine der folgenden Schaltflächen klicken:

   - **Programm beenden**

     Diese Schaltfläche ist nur verfügbar, wenn das Programm gerade ausgeführt wird.

   - **Programm neu starten**

     Diese Schaltfläche ist nur verfügbar, wenn das Programm gerade ausgeführt wird.

   - **Programm starten**

     Diese Schaltfläche ist nur verfügbar, wenn das Programm derzeit nicht ausgeführt wird.

Je nach ausgewählter Aktion wird das erforderliche Programm auf dem Client-Gerät gestartet, beendet oder neu gestartet.

Wenn Sie den Administrationsagenten neu starten, wird eine Meldung angezeigt, dass die aktuelle Verbindung des Geräts zum Administrationsserver unterbrochen wird.

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 **Programme von Kaspersky** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Programme angezeigt.

3. Wählen Sie in der Liste der Programme jenes aus, für das Sie die 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. Sie müssen das Programm nicht auf dem Gerät installieren.

Gehen Sie wie folgt vor, um ein Programm auf dem Client-Gerät auszuführen:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.

2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Remote-Anwendung ausführen** aus.

3. Klicken Sie im Abschnitt **Programmdateien** auf die Schaltfläche **Durchsuchen**, um ein zip-Archiv auszuwählen, das die Anwendung enthält, die Sie auf dem Client-Gerät ausführen möchten.

   > Das zip-Archiv muss den Ordner mit dem Tool enthalten. In diesem Ordner befindet sich die ausführbare Datei, die auf einem Remote-Gerät ausgeführt werden soll.

   Bei Bedarf können Sie den Namen der ausführbaren Datei und die Befehlszeilenargumente angeben. Füllen Sie dazu die Felder **Archivierte ausführbare Datei, die auf einem Remote-Gerät ausgeführt werden soll** und **Argumente der Befehlszeile** aus.

4. Klicken Sie auf die Schaltfläche **Hochladen und ausführen**, um die angegebene Anwendung auf einem Client-Gerät auszuführen.

5. Folgen Sie den Anweisungen des Experten vom Kaspersky-Support.

Erzeugen einer Dump-Datei für eine Anwendung

Mit einer Dump-Datei für eine Anwendung können Sie die Parameter der Anwendung anzeigen, die an einem bestimmten Zeitpunkt auf einem Client-Gerät ausgeführt wird. Diese Datei enthält auch Informationen über die Module, die für eine Anwendung geladen wurden.

Das Generieren von Dump-Dateien ist nur für 32-Bit-Prozesse verfügbar, die auf Windows-basierten Client-Geräten ausgeführt werden. Für 64-Bit-Prozesse wird diese Funktion 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-Anwendung ausführen** 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 Security Center Cloud Console 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 **Geräte → Verwaltete Geräte.**

2. Aktivieren Sie das Kontrollkästchen neben dem Namen des Geräts, für das Sie Zugriff benötigen.

3. Klicken Sie auf die Schaltfläche **Remotedesktopverbindung herstellen**.

   Das Fenster "Remotedesktop (nur Windows)" 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 "Remotedesktop (nur Windows)" 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 **Geräte** → **Verwaltete 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 Adaptive Kontrolle von Anomalien und Funden, die von Regeln für die Adaptive Kontrolle von Anomalien in Kaspersky Endpoint Security für Windows auf Client-Geräten durchgeführt wird.

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 Security Center Cloud Console. Diese Informationen werden als Liste im Unterordner **Auslösen von Regeln im Smart-Training-Status** des Ordners **Datenverwaltung** gespeichert. Sie können Funde als korrekt bestätigen oder sie als Ausschlüsse hinzufügen, damit solches Verhalten in der Zukunft nicht als anomal 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 **Auslösen von Regeln 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 dem die Regel übernommen wurde.

   - **Name**

     Name der Regel, die übernommen wurde.

   - **Status**

Ausschluss wird erstellt – Wenn der Administrator dieses Element verarbeitet und als Ausschluss aus den 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.

Bestätigung – 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. zum Prozess, der diese Aktion durchführt (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Hash des Quellprozesses**

  SHA-256-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**

  SHA-256-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**

  SHA-256-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**

  SHA-256-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 **Auslösen von Regeln 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.

Um ein Element zu bestätigen, gehen Sie wie folgt vor:

Klicken Sie auf ein Element (oder mehrere Elemente) in der Liste der Funde und anschließend auf die Schaltfläche **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 Anweisungen 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** → **Auslösen von Regeln 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, sie zu den Ausschlüssen hinzuzufügen, wird eine Fehlermeldung angezeigt.

Daraufhin wird der Assistent für das Hinzufügen eines Ausschlusses gestartet.

Richtlinien und Richtlinienprofile

In Kaspersky Security Center Cloud Console können Sie Richtlinien für Programme von Kaspersky erstellen. In diesem Abschnitt werden Richtlinien und Richtlinienprofile beschrieben, und Sie erhalten Anweisungen für deren Erstellung und Änderung.

Über Richtlinien

Eine *Richtlinie* besteht aus einer Reihe von Kaspersky-Programmeinstellungen, die auf eine Administrationsgruppe und deren Untergruppen angewendet werden. Sie können mehrere Kaspersky-Programme auf den Geräten einer Administrationsgruppe installieren. Kaspersky Security Center Cloud Console bietet eine Richtlinie für jedes Kaspersky-Programm 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 ein Kaspersky-Programm aktiv sein. Geräte wenden die Einstellungswerte einer aktiven Richtlinie für ein Kaspersky-Programm 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 ein einzelnes Programm 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 Virenepidemien 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 lokale Programmeinstellungen 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 ein Sperrschaltflächensymbol (🔒). Die folgende Tabelle zeigt den Status der Sperrschaltfläche:

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 verwalteten Programmoberfläche 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 eines verwalteten Programms 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-Programmen auf verwalteten Geräten geändert werden.

Sie können eine Sperrschaltfläche verwenden, um die folgenden Aktionen auszuführen:

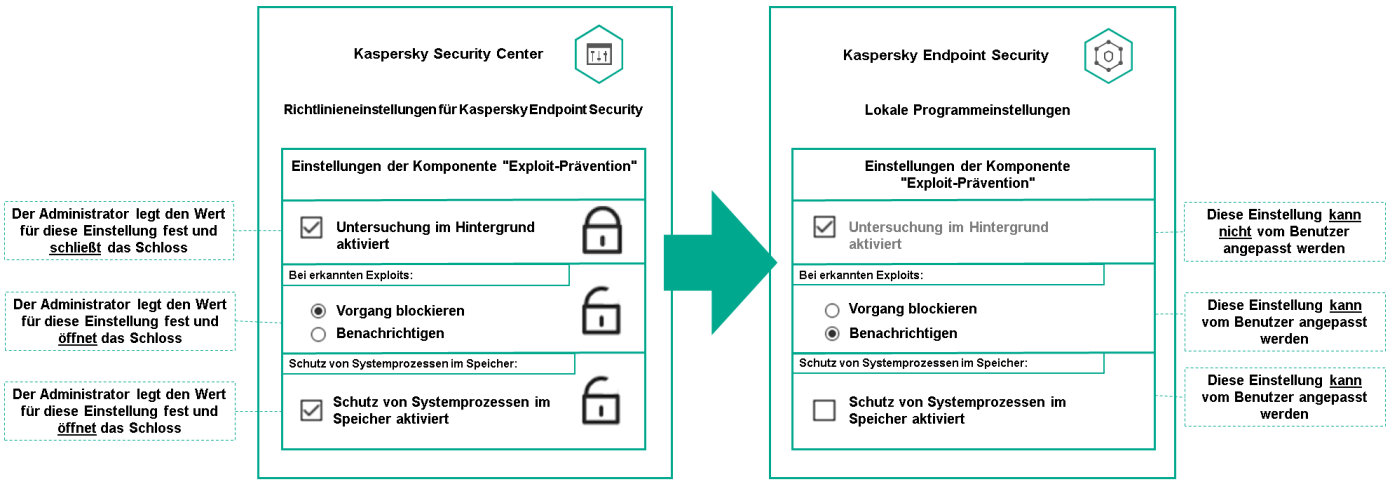
- Sperren von Einstellungen für eine Verwaltungsuntergruppenrichtlinie
- Sperren von Einstellungen eines Kaspersky-Programms auf einem verwalteten Gerät

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 ein verwaltetes Kaspersky-Programm enthalten dieselben Einstellungen. Wenn Sie Richtlinieneinstellungen konfigurieren, ändern die Einstellungen des Kaspersky-Programms die Werte auf einem verwalteten Gerät. Sie können gesperrte Einstellungen auf einem verwalteten Gerät nicht anpassen (siehe Abbildung unten):



Einzelheiten zu den Einstellungen der Kaspersky-Programme

Vererbung von Richtlinien und Richtlinienprofilen

Dieser Abschnitt enthält Informationen zur Hierarchie und Vererbung von Richtlinien und Richtlinienprofilen.

Hierarchie der Richtlinien

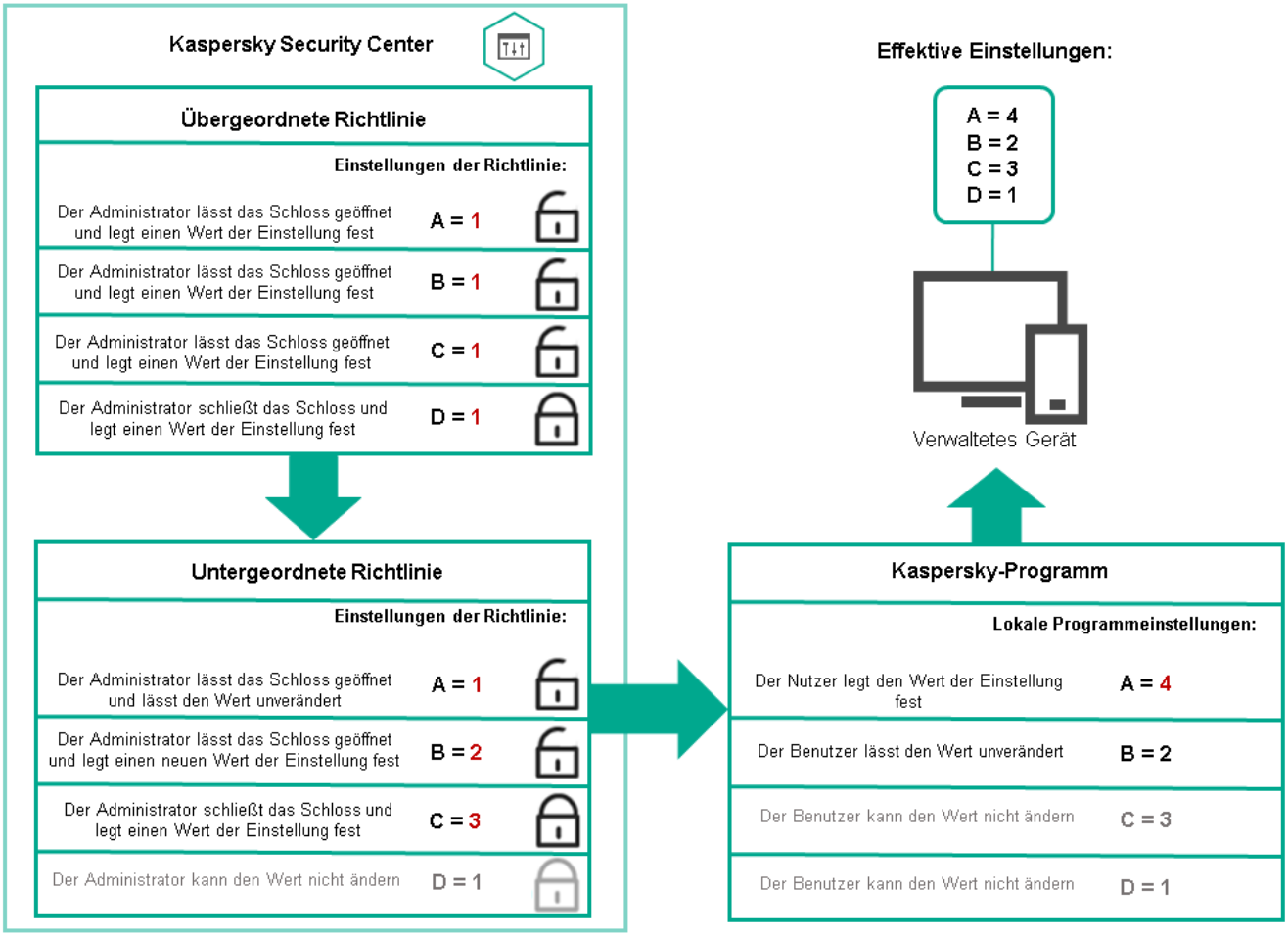
Wenn unterschiedliche Geräte unterschiedliche Einstellungen benötigen, können Sie Geräte in Administrationsgruppen organisieren.

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 desselben Programms 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).

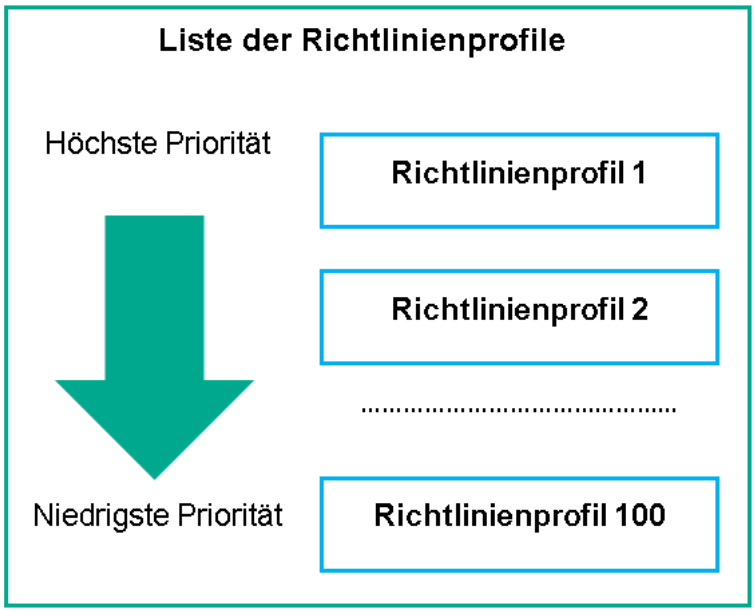


Hierarchie der Richtlinien

Richtlinienprofile in einer Hierarchie von Richtlinien

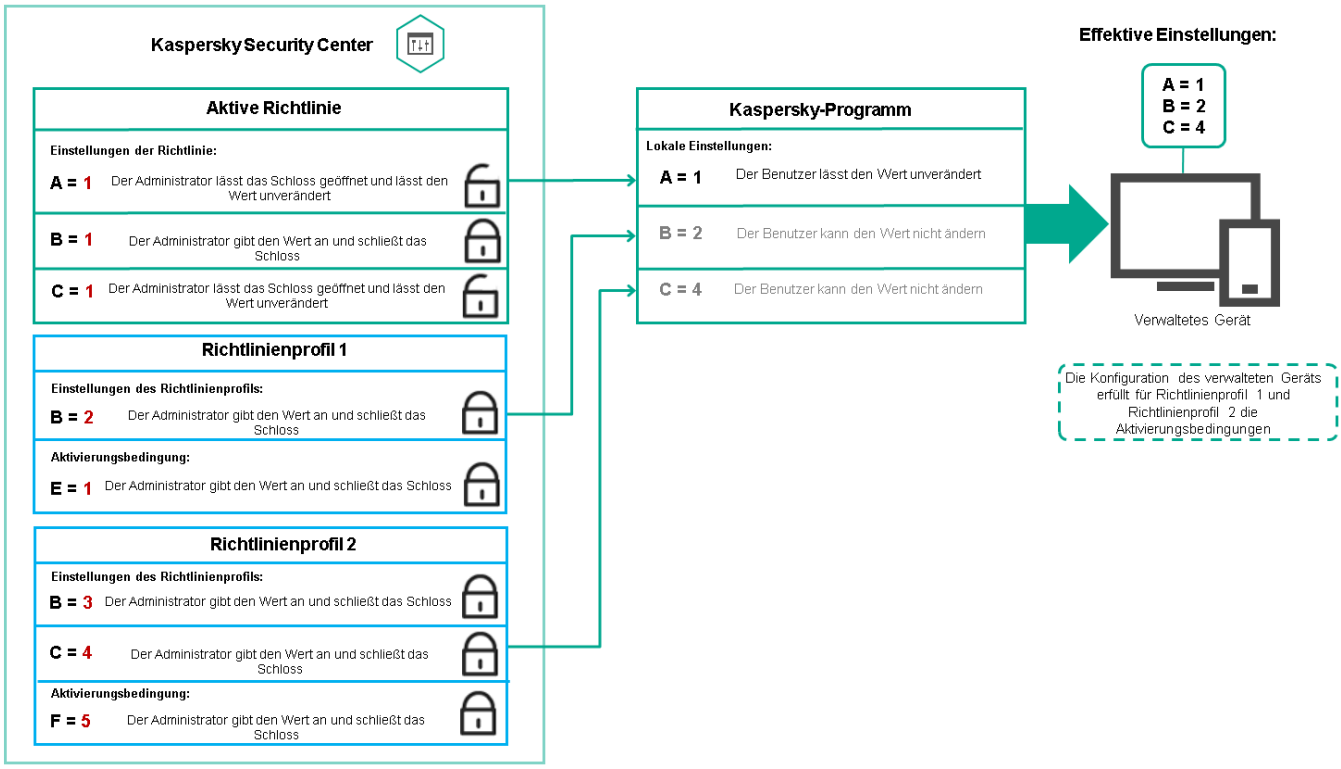
Richtlinienprofile haben die folgenden Bedingungen für die Prioritätszuweisung:

- 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.

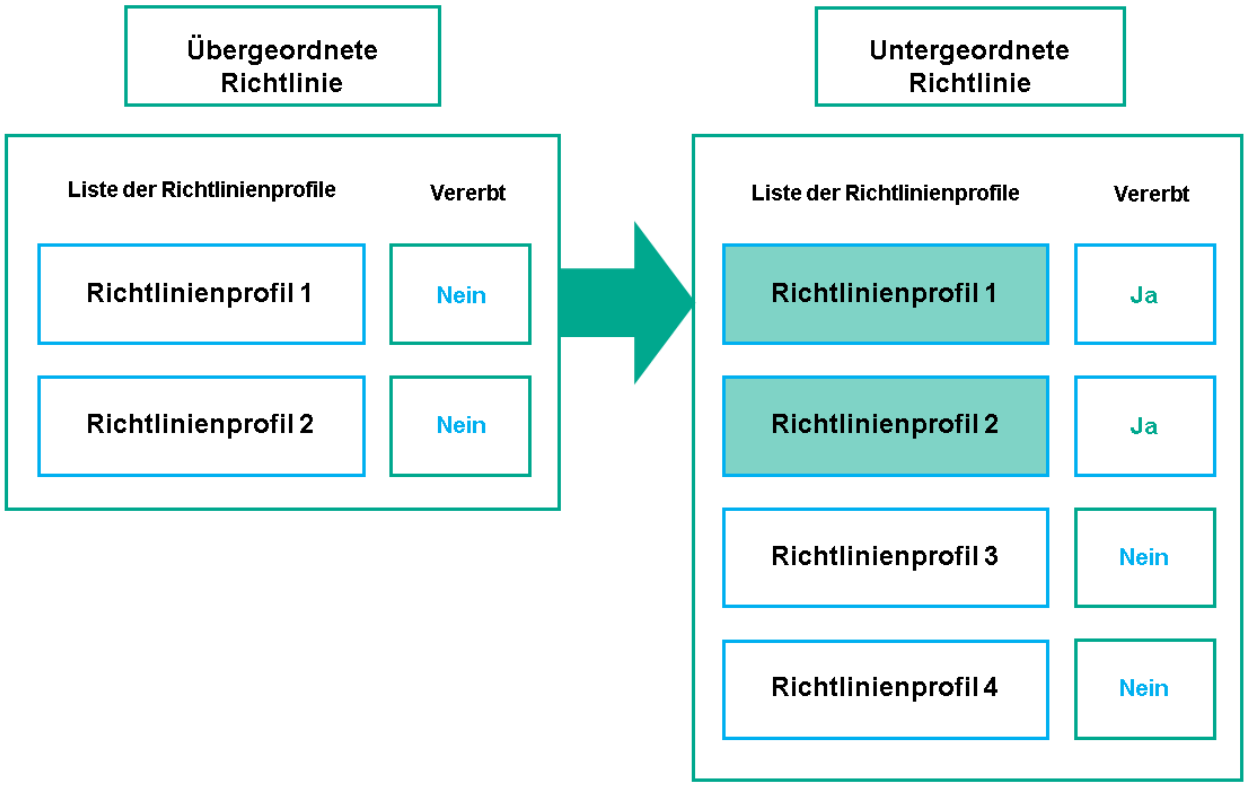
Richtlinienprofile in einer Vererbungshierarchie

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).

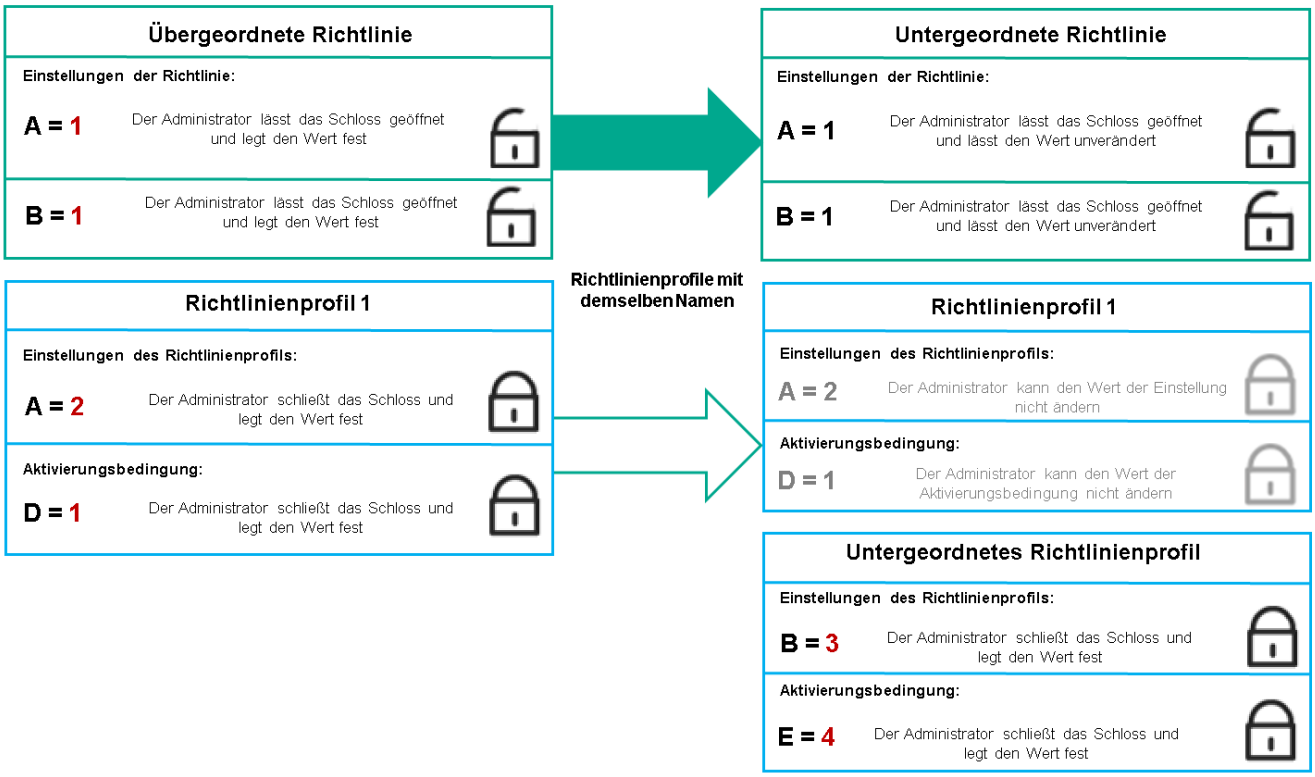


Vererbung von Richtlinienprofilen

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 des verwalteten Programms 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. Wechseln Sie im Hauptmenü zu **Geräte** → **Gruppenhierarchie**.
2. Wählen Sie in der Struktur der Administrationsgruppe die Administrationsgruppe aus, für welche Sie die Liste mit Richtlinien anzeigen möchten.

Daraufhin wird die Liste der Richtlinien in Tabellenformat geöffnet. Wenn noch keine Richtlinien existieren, ist die Tabelle leer. Sie können die Spalten der Tabelle ein- und ausblenden, ihre Reihenfolge verändern, nur Zeilen mit einem bestimmten Wert anzeigen und die Suchfunktion verwenden.

Richtlinie erstellen

Sie können Richtlinien erstellen sowie Sie bestehende Richtlinien ändern und löschen.

Sie können keine Administrationsserver-Richtlinie erstellen.

Um eine Richtlinie zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Richtlinien und Profile**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Programm auswählen** wird geöffnet.
3. Wählen Sie das Programm aus, für das Sie eine Richtlinie erstellen möchten.
4. Klicken Sie auf die Schaltfläche **Weiter**.

   Das Fenster für neue Richtlinieneinstellungen wird geöffnet, in dem die Registerkarte **Allgemein** ausgewählt ist.
5. Ändern Sie gegebenenfalls Standardname, Standardstatus und Standardvererbungseinstellungen der Richtlinie.
6. Klicken Sie auf die Registerkarte **Programmeinstellungen**.

   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.
7. Wählen Sie auf der Registerkarte **Programmeinstellungen** im linken Bereich die gewünschte Kategorie aus und ändern Sie im Ergebnisbereich auf der rechten Seite die Einstellungen der Richtlinie. Sie können die Einstellungen der Richtlinie in jeder Kategorie (jedem Abschnitt) ändern.

   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.

8. 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 **Geräte** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie, die Sie ändern möchten.

   Das Fenster mit den Richtlinieneinstellungen wird geöffnet.
3. Geben Sie die Allgemeinen Einstellungen und Einstellungen des Programms an, für welches Sie eine Richtlinie erstellen. Weitere Informationen finden Sie hier:

   - Administrationsserver-Konfiguration
   - Richtlinieneinstellungen des Administrationsagenten
   - Dokumentation zu Kaspersky Endpoint Security für Windows

   Ausführliche Informationen über die Einstellungen anderer Sicherheitsanwendungen finden Sie in der Dokumentation zu dieser Anwendung.
4. Klicken Sie auf die Schaltfläche **Speichern**.

Die Änderungen der Richtlinie werden in den Eigenschaften der Richtlinie gespeichert und im Abschnitt **Revisionsverlauf** angezeigt.

Allgemeine Richtlinieneinstellungen

Allgemein

Auf der Registerkarte **Allgemein** können Sie den Richtlinienstatus ändern und die Vererbung der Richtlinieneinstellungen anpassen:

- Im Block **Richtlinienstatus** können Sie einen der Richtlinienmodi auswählen:
  - **Aktiv**
  - **Mobil**

Bei Auswahl dieser Option wird die Richtlinie aktiv, sobald das Gerät vom Unternehmensnetzwerk getrennt wird.

- **Inaktiv**

  Bei Auswahl dieser Option wird die Richtlinie inaktiv, aber im Ordner **Richtlinien** gespeichert. Bei Bedarf kann die Richtlinie aktiviert werden.

- In der Einstellungsgruppe **Einstellungen erben** können Sie Einstellungen für die Vererbung der Richtlinie anpassen:

  - **Einstellungen aus übergeordneter Richtlinie erben**

    Ist diese Option aktiviert, so werden die Werte der Richtlinieneinstellungen aus der Richtlinie der obersten Hierarchie-Ebene vererbt und können nicht geändert werden.

    Diese Option ist standardmäßig aktiviert.

  - **Vererben der Einstellungen für untergeordnete Richtlinien erzwingen**

    Ist diese Option aktiviert, so werden die folgenden Aktionen ausgeführt, nachdem die Richtlinienänderungen übernommen wurden:

    - Einstellungen der Richtlinie werden in die Tochter-Richtlinien, d.h. in die Richtlinien der untergeordneten Administrationsgruppen, übertragen.
    - Im Block **Einstellungen erben** des Abschnitts **Allgemein** im Eigenschaftenfenster aller untergeordneten Richtlinien wird die Option **Einstellungen aus Richtlinie der höheren Ebene erben** automatisch aktiviert.

    Ist diese Option aktiviert, so können die Einstellungen der untergeordneten Richtlinien nicht geändert werden.

    Diese Option ist standardmäßig deaktiviert.

Konfiguration von Ereignissen

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.

Revisionsverlauf

Auf der Registerkarte **Revisionsverlauf** können Sie eine Liste mit Revisionen der Richtlinie anzeigen und bei Bedarf ein Rollback der Änderungen an der Richtlinie vornehmen.

Aktivieren und Deaktivieren einer Richtlinienvererbungsoption

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 **Vererben der Einstellungen für untergeordnete Richtlinien erzwingen** in der übergeordneten Gruppe aktivieren, wird dadurch **Einstellungen aus übergeordneter Richtlinie erben** für alle untergeordneten Richtlinien aktiviert. In diesem Fall kann diese Option nicht für untergeordnete Richtlinien deaktiviert werden. Alle Einstellungen, die in der übergeordneten Richtlinie gesperrt sind, werden zwangsweise an untergeordnete Gruppen vererbt und können in den untergeordneten Gruppen nicht bearbeitet werden.

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 **Geräte** → **Richtlinien und Profile**.
2. Aktivieren Sie die Kontrollkästchen neben der Richtlinie (oder den Richtlinien), die Sie kopieren möchten.
3. Klicken Sie auf die Schaltfläche **Kopieren**.

   Im rechten Bereich des Bildschirms erscheint die Strukturansicht der Administrationsgruppen.
4. Wählen Sie in der Strukturansicht die Zielgruppe aus. Das ist die Gruppe, zu der Sie die Richtlinie (oder die Richtlinien) kopieren möchten.
5. Klicken Sie auf die Schaltfläche **Kopieren** am unteren Rand des Bildschirms.
6. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Die Richtlinie bzw. Richtlinien werden samt allen Profilen zur Zielgruppe kopiert. Der Status jeder kopierten Richtlinie in der Zielgruppe ist **Inaktiv**. Sie können den Status jederzeit auf **Aktiv** setzen.

Wenn die gewählte Richtlinienliste bereits eine Richtlinie mit dem gleichen Namen wie die zu verschiebende Richtlinie enthält, wird dem Namen der verschobenen Richtlinie eine Endung der Form (<laufende Nummer>) angehängt. Beispiel: (1).

Richtlinie verschieben

Richtlinien können von einer Administrationsgruppe zu einer anderen verschoben werden. Angenommen, Sie möchten eine Gruppe löschen, aber ihre Richtlinien für eine andere Gruppe verwenden. In diesem Fall können Sie die Richtlinie der alten Gruppe zur neuen Gruppe verschieben, bevor Sie die Gruppe löschen.

Um eine Richtlinie zu einer anderen Administrationsgruppe zu verschieben, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Richtlinien und Profile**.
2. Aktivieren Sie die Kontrollkästchen neben der Richtlinie (oder den Richtlinien), die Sie verschieben möchten.
3. Klicken Sie auf die Schaltfläche **Verschieben**.

   Im rechten Bereich des Bildschirms erscheint die Strukturansicht der Administrationsgruppen.
4. Wählen Sie in der Strukturansicht die Zielgruppe aus. Das ist die Gruppe, zu der Sie die Richtlinie (oder die Richtlinien) verschieben möchten.
5. Klicken Sie auf die Schaltfläche **Verschieben** am unteren Rand des Bildschirms.
6. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Wenn die Richtlinie nicht von der Quellgruppe geerbt wurde, wird sie samt allen Profilen zur Zielgruppe verschoben. Der Status der Richtlinie in der Zielgruppe ist **Inaktiv**. Sie können den Status jederzeit auf **Aktiv** setzen.

Wenn die Richtlinie von der Quellgruppe geerbt wurde, bleibt sie in der Quellgruppe erhalten. Sie wird samt allen Profilen zur Zielgruppe kopiert. Der Status der Richtlinie in der Zielgruppe ist **Inaktiv**. Sie können den Status jederzeit auf **Aktiv** setzen.

Wenn die gewählte Richtlinienliste bereits eine Richtlinie mit dem gleichen Namen wie die zu verschiebende Richtlinie enthält, wird dem Namen der verschobenen Richtlinie eine Endung der Form (<laufende Nummer>) angehängt. Beispiel: (1).

Richtlinien exportieren

Mit Kaspersky Security Center Cloud Console 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 **Geräte** → **Richtlinien und Profile**.
2. Aktivieren Sie das Kontrollkästchen neben der Richtlinie, die Sie installieren möchten.

   Sie können nicht mehrere Richtlinien gleichzeitig exportieren. Wenn Sie mehr als eine Richtlinie auswählen, wird die Schaltfläche **Exportieren** deaktiviert.
3. Klicken Sie auf die Schaltfläche **Exportieren**.
4. Geben Sie im folgenden Fenster **Speichern unter** den Namen und den Pfad der Richtliniendatei an. Klicken Sie auf **Speichern**.

   Das Fenster **Speichern unter** wird nur angezeigt, wenn Sie Google Chrome, Microsoft Edge oder Opera verwenden. Wenn Sie einen anderen Browser verwenden, wird die Richtliniendatei automatisch im Ordner **Downloads** gespeichert.

Richtlinien importieren

Mit Kaspersky Security Center Cloud Console 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 **Geräte** → **Richtlinien und Profile**.
2. Klicken Sie auf die Schaltfläche **Importieren**.
3. Klicken Sie auf die Schaltfläche **Durchsuchen**, um eine Richtliniendatei auszuwählen, die Sie importieren möchten.
4. Geben Sie im folgenden Fenster den Pfad zur klp-Richtliniendatei an und klicken Sie anschließend auf die Schaltfläche **Öffnen**. Beachten Sie, dass Sie nur eine Richtliniendatei auswählen können.

Die Verarbeitung der Richtlinien beginnt.

5. Nachdem die Richtlinie erfolgreich verarbeitet wurde, wählen Sie die Administrationsgruppe aus, auf die Sie die Richtlinie anwenden möchten.

6. Klicken Sie auf die Schaltfläche **Abgeschlossen**, um den Import der Richtlinie abzuschließen.

Die Benachrichtigung mit dem Resultat des Imports wird angezeigt. Wenn die Richtlinie erfolgreich importiert wurde, können Sie zum Anzeigen der Eigenschaften der Richtlinie auf den Link **Details** klicken.

Nach einem erfolgreichem Import wird die Richtlinie in der Liste der Richtlinien angezeigt. Die Einstellungen und Profile der Richtlinie werden ebenfalls importiert. Unabhängig vom Richtlinienstatus, der während des Exports ausgewählt wurde, ist die importierte Richtlinie inaktiv. Sie können den Richtlinienstatus in den Eigenschaften der Richtlinie ändern.

Wenn die neu importierte Richtlinie denselben Namen wie eine bereits vorhandene Richtlinie besitzt, wird der Name der importierten Richtlinie um den Index **(<nächste Sequenznummer>)** erweitert, zum Beispiel: **(1)**, **(2)**.

Anzeigen des Statusdiagramms für die Richtlinienverteilung

In Kaspersky Security Center Cloud Console 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. Wechseln Sie im Hauptmenü zu **Geräte** → **Richtlinien und Profile**.

2. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie, für die Sie den Verteilungsstatus auf dem Gerät anzeigen wollen.

3. 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. Wechseln Sie im Hauptmenü zu Ihren Kontoeinstellungen und wählen Sie anschließend **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 eine Richtlinie beim Eintritt eines Ereignisses "Virenangriff" automatisch aktiviert wird, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Fenster für die Einstellungen des Administrationsservers wird geöffnet und Registerkarte **Allgemein** ist ausgewählt.

2. Wählen Sie den Bereich **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 für die Komponente, die den Virenangriff erkannt hat – Anti-Virus für Workstations und Server, Antiviren-Programme für E-Mail-Systeme, 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 Richtungspfeil (>) neben **Verwaltete Geräte**.

   Eine Hierarchie der Administrationsgruppen und ihrer Richtlinien wird angezeigt.

6. Klicken Sie in der Hierarchie der Administrationsgruppen und ihrer Richtlinien auf die Namen der Richtlinien, die aktiviert werden, wenn ein Virenangriff erkannt wird.

   Um sämtliche Richtlinien in der Liste oder in einer Gruppe auszuwählen, aktivieren Sie das Kontrollkästchen neben dem benötigten Namen.

7. Klicken Sie auf die Schaltfläche **Speichern**.

   Das Fenster mit der Hierarchie der Administrationsgruppen und ihrer Richtlinien wird geschlossen.

Die ausgewählten Richtlinien werden in die Liste der Richtlinien aufgenommen, die aktiviert werden, wenn ein Virenangriff erkannt wird. Die ausgewählten Richtlinien werden bei einem Virenangriff 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 Security Center Cloud Console 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.

Synchronisation eines einzelnen Geräts

So erzwingen Sie die Synchronisierung zwischen dem Administrationsserver und dem verwalteten Gerät:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte**.
2. Klicken Sie auf den Namen des Geräts, das mit dem Administrationsserver synchronisiert werden soll.
   Ein Eigenschaftenfenster wird geöffnet, in dem der Abschnitt **Allgemein** ausgewählt ist.
3. Klicken Sie auf die Schaltfläche **Synchronisierung erzwingen**.

Die Anwendung synchronisiert das ausgewählte Gerät mit dem Administrationsserver.

Synchronisation mehrerer Geräte

So erzwingen Sie die Synchronisierung zwischen dem Administrationsserver und mehreren verwalteten Geräten:

1. Öffnen Sie die Geräteliste einer Administrationsgruppe oder einer Geräteauswahl:
   - Wechseln Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte** → **Gruppen** und wählen Sie anschließend die Administrationsgruppe aus, welche die zu synchronisierenden Geräte enthält.
   - Führen Sie eine Geräteauswahl durch, um die Geräteliste anzuzeigen.
2. Aktivieren Sie die Kontrollkästchen neben den Geräten, die Sie mit dem Administrationsserver synchronisieren möchten.
3. Klicken Sie auf die Schaltfläche **Synchronisierung erzwingen**.
   Das Programm 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 ein Kaspersky-Programm 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 Programmrichtlinie an ein verwaltetes Gerät übermittelt wurde:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte**.
2. Klicken Sie auf den Namen des Geräts, das mit dem Administrationsserver synchronisiert werden soll.
   Ein Eigenschaftenfenster wird geöffnet, in dem der Abschnitt **Allgemein** ausgewählt ist.
3. Klicken Sie auf die Registerkarte **Programme**.
4. Wählen Sie das Programm aus, für das Sie das Datum der Richtliniensynchronisierung anzeigen möchten.

Das Fenster mit der Programmrichtlinie wird geöffnet; dabei ist der Abschnitt **Allgemein** ausgewählt und das Datum und die Uhrzeit der Übertragung der Richtlinie werden angezeigt.

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 **Geräte** → **Richtlinien und Profile**.
2. Aktivieren Sie die Kontrollkästchen neben der Richtlinie, die Sie löschen möchten, und klicken Sie auf **Löschen**.

   Die Schaltfläche **Löschen** ist nicht verfügbar (abgeblendet), wenn Sie eine geerbte Richtlinie auswählen.
3. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Die Richtlinie wird samt allen Profilen gelöscht.

Richtlinienprofile verwalten

Dieser Abschnitt beschreibt die Verwaltung von Richtlinienprofilen und enthält Informationen zum Anzeigen der Profile einer Richtlinie, zum Ändern einer Richtlinienprofilpriorität, zum Erstellen eines Richtlinienprofils, zum Ändern eines Richtlinienprofils, zum Kopieren eines Richtlinienprofils, zum Erstellen einer Richtlinienprofilaktivierungsregel und zum Löschen eines Richtlinienprofils.

Anzeigen der Profile einer Richtlinie

So zeigen Sie Profile einer Richtlinie an:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Richtlinien und Profile**.
2. Klicken Sie auf den Namen der Richtlinie, deren Profile Sie anzeigen möchten.

   Das Fenster mit den Eigenschaften der Richtlinie wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.
3. Öffnen Sie die Registerkarte **Richtlinienprofile**.

Daraufhin wird die Liste der Richtlinienprofile in Tabellenformat geöffnet. Wenn die Richtlinie über keine Profile verfügt, wird eine leere Tabelle angezeigt.

Priorität eines Richtlinienprofils ändern

Um die Priorität eines Richtlinienprofils zu ändern, gehen Sie wie folgt vor:

1. 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, dessen Priorität Sie ändern möchten.

3. Ändern Sie die Position des Richtlinienprofils in der Liste, indem Sie auf **Priorisieren** oder **Priorisierung verringern** klicken.

   Je höher ein Richtlinienprofil in der Liste steht, desto höher ist seine Priorität.

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

Die Priorität des ausgewählten Richtlinienprofils wird verändert und angewendet.

Richtlinienprofil erstellen

Um ein Richtlinienprofil zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet. Wenn die Richtlinie über keine Profile verfügt, wird eine leere Tabelle angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

3. Ändern Sie gegebenenfalls den Standardnamen und die Standardvererbungseinstellungen des Profils.

4. Wählen Sie die Registerkarte **Programmeinstellungen** aus.

   Alternativ dazu können Sie auf **Speichern** klicken und beenden. Das Profil, das Sie erstellt haben, wird in der Liste der Richtlinienprofile angezeigt, und Sie können seine Einstellungen später anpassen.

5. Wählen Sie auf der Registerkarte **Programmeinstellungen** im linken Bereich die gewünschte Kategorie aus und ändern Sie im Ergebnisbereich auf der rechten Seite die Einstellungen für das Profil. Sie können die Einstellungen des Richtlinienprofils in jeder Kategorie (jedem Abschnitt) ändern.

   Beim Ändern der Einstellungen können Sie auf **Abbrechen** klicken, um den letzten Vorgang rückgängig zu machen.

6. Klicken Sie auf **Speichern**, um das Profil zu speichern.

Das Profil wird in der Liste der Richtlinienprofile angezeigt.

Richtlinienprofil ändern

Richtlinienprofile können nur für Richtlinien von Kaspersky Endpoint Security für Windows geändert werden.

Um die Einstellungen eines Richtlinienprofils zu ändern, gehen Sie wie folgt vor:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet.

2. Wählen Sie auf der Registerkarte **Richtlinienprofile** das Richtlinienprofil aus, das Sie bearbeiten möchten.

   Daraufhin wird das Eigenschaftenfenster des Richtlinienprofils geöffnet.

3. Passen Sie im Eigenschaftenfenster die Einstellungen des Profils an:

   - Ändern Sie auf der Registerkarte **Allgemein** bei Bedarf den Namen des Profils und aktivieren bzw. deaktivieren Sie das Profil.
   - Bearbeiten Sie die Regeln für die Profilaktivierung.
   - Programmeinstellungen bearbeiten.

   Ausführliche Informationen über die Einstellungen von Sicherheitsanwendungen finden Sie in der Dokumentation der entsprechenden Anwendung.

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

Die geänderten Einstellungen werden nach der Synchronisierung des Geräts mit dem Administrationsserver (wenn das Richtlinienprofil aktiv ist) bzw. nach der Ausführung der Aktivierungsregeln (wenn das Richtlinienprofil nicht aktiv ist) angewendet.

Richtlinienprofil kopieren

Sie können ein Richtlinienprofil zur aktuellen oder zu einer anderen Richtlinie kopieren, wenn Sie z. B. identische Profile für verschiedene Richtlinien festlegen möchten. Das Kopieren von Profilen ist auch dann nützlich, wenn Sie zwei oder mehrere Profile anlegen möchten, deren Einstellungen sich nur minimal unterscheiden.

Um ein Richtlinienprofil zu kopieren, gehen Sie wie folgt vor:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet. Wenn die Richtlinie über keine Profile verfügt, wird eine leere Tabelle angezeigt.

2. Wählen Sie auf der Registerkarte **Richtlinienprofile** das Richtlinienprofil aus, das Sie kopieren möchten.

3. Klicken Sie auf die Schaltfläche **Kopieren**.

4. Wählen Sie im nächsten Fenster die Richtlinie aus, zu der Sie das Profil kopieren möchten.

   Das Richtlinienprofil kann zur gleichen Richtlinie oder zu einer von Ihnen angegebenen Richtlinie kopiert werden.

5. Klicken Sie auf die Schaltfläche **Kopieren**.

   Das Richtlinienprofil wird zur festgelegten Richtlinie kopiert. Dem zuletzt kopierten Profil wird die niedrigste Priorität zugewiesen. Wenn Sie das Profil zur selben Richtlinie kopieren, wird dem neu kopierten Profil der Index () angehängt, z. B. (1), (2).

Die Einstellungen des Profils, einschließlich Name und Priorität, können später geändert werden; das ursprüngliche Richtlinienprofil ändert sich in diesem Fall nicht.

Regeln für die Aktivierung des Richtlinienprofils erstellen

Um eine Regel für die Aktivierung des Richtlinienprofils zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet.

2. Wählen Sie auf der Registerkarte **Richtlinienprofile** das Richtlinienprofil aus, für das Sie eine Aktivierungsregel anlegen möchten.

   Wenn die Richtlinienprofilliste leer ist, können Sie ein Richtlinienprofil erstellen.

3. Klicken Sie auf der Registerkarte **Aktivierungsregeln** auf die Schaltfläche **Hinzufügen**.

   Das Fenster mit Regeln für die Aktivierung des Richtlinienprofils wird geöffnet.

4. Geben Sie einen Namen für die Regel ein.

5. Aktivieren Sie die Kontrollkästchen neben den Bedingungen, die Einfluss auf die Aktivierung des erstellten Richtlinienprofils haben sollen:

   - **Allgemeine Regeln für die Aktivierung des Richtlinienprofils**

     Aktivieren Sie das Kontrollkästchen, um die Regeln für die Aktivierung des Richtlinienprofils auf dem Gerät je nach dem Zustand des autonomen Modus des Geräts, der Verbindungsregel des Geräts mit dem Administrationsserver und den dem Gerät zugewiesenen Tags anzupassen.

     Geben Sie für diese Option im nächsten Schritt Folgendes an:

     - **Gerätestatus**

       Legt die Bedingung für die Verfügbarkeit des Geräts im Netzwerk fest:

       - **Online** – Das Gerät befindet sich im Netzwerk und somit ist der Administrationsserver ist verfügbar.
       - **Autonom** – Das Gerät befindet sich in einem externen Netzwerk, daher ist der Administrationsserver nicht verfügbar.
       - **N/A** – Das Kriterium wird nicht angewendet.

   - **Die Regel für die Verbindung des Administrationsservers ist auf diesem Gerät aktiv**

     Wählen Sie die Aktivierungsbedingung für das Richtlinienprofil (Regel wird erfüllt bzw. nicht erfüllt) und bestimmen Sie den Regelnamen.

     Die Regel definiert den Netzwerkspeicherort des Geräts für die Verbindung mit dem Administrationsserver; bei Erfüllen bzw. Nichterfüllen ihrer Bedingungen wird das Richtlinienprofil aktiviert.

     Die Beschreibung des Netzwerkspeicherorts der Geräte für die Verbindung mit dem Administrationsserver kann erstellt oder in der Regel für die Umschaltung des Administrationsagenten angepasst werden.

- **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 Security Center Cloud Console 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 Security Center Cloud Console angeben. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

- **Regeln für Hardware-Eigenschaften**

  Aktivieren Sie das Kontrollkästchen, um auf dem Gerät die Aktivierung der Richtlinienprofile je nach Speichergröße und Anzahl seiner logischen Prozesse anzupassen.

  Geben Sie für diese Option im nächsten Schritt Folgendes an:

  - **Arbeitsspeichergröße (MB)**

Aktivieren Sie diese Option, um die Regel zur Aktivierung des Profils auf dem Gerät anhand der Arbeitsspeichergröße des Geräts anzupassen und zu aktivieren. In der Dropdown-Liste unter diesem Kontrollkästchen können die Kriterien für die Aktivierung des Profils ausgewählt werden:

- Arbeitsspeicher des Geräts kleiner als festgelegter Wert (Zeichen "<")
- Arbeitsspeicher des Geräts größer als festgelegter Wert (Zeichen ">")

Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt. Sie können die Größe des Arbeitsspeichers auf dem Gerät angeben. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

- Anzahl der logischen Prozessoren

Aktivieren Sie diese Option, um die Regel zur Aktivierung des Profils auf dem Gerät anhand der Anzahl der logischen Prozessoren des Geräts anzupassen und zu aktivieren. In der Dropdown-Liste unter diesem Kontrollkästchen können die Kriterien für die Aktivierung des Profils ausgewählt werden:

- Anzahl der logischen Prozesse des Geräts kleiner oder gleich festgelegter Wert (Zeichen "<")
- Anzahl der logischen Prozesse des Geräts größer oder gleich festgelegter Wert (Zeichen ">")

Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt. Sie können die Anzahl der logischen Prozessoren auf dem Gerät angeben. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

- **Regeln für Rollenzuordnung**

  Geben Sie für diese Option im nächsten Schritt Folgendes an:

  Richtlinienprofil durch eine bestimmte Rolle des Gerätebesitzers aktivieren

  Aktivieren Sie diese Option, um die Regel zur Aktivierung des Profils auf dem Gerät in Abhängigkeit von der Rolle des Besitzers zu konfigurieren. Fügen Sie die Rolle manuell aus der Liste vorhandener Rollen hinzu.

  Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt.

- Regeln zur Verwendung von Tags

  Aktivieren Sie das Kontrollkästchen, um die Regeln für die Aktivierung des Richtlinienprofils auf dem Gerät abhängig von den Tags anzupassen, die dem Gerät zugewiesen wurden. Sie können das Richtlinienprofil entweder für alle Geräte mit diesem Tag oder alle Geräte ohne dieses Tag aktivieren.

  Geben Sie für diese Option im nächsten Schritt Folgendes an:

  - Tag

Geben Sie in der Liste der Tags Aktivierungsregeln für Geräte im Richtlinienprofil an, indem Sie die Kontrollkästchen der entsprechenden Tags aktivieren.

Sie können neue Tags zur Liste hinzufügen, indem Sie diese im Feld über der Liste eingeben und auf die Schaltfläche **Hinzufügen** klicken.

Das Richtlinienprofil erstreckt sich auf Geräte, in deren Beschreibung alle ausgewählten Tags vorkommen. Sind Kontrollkästchen deaktiviert, wird das Kriterium nicht angewandt. Standardmäßig sind die Kontrollkästchen deaktiviert.

- **Auf Geräte ohne angegebene Tags anwenden**

  Aktivieren Sie die Option, wenn die Auswahl der Tags invertiert werden muss.

  Wenn diese Option aktiviert ist, werden Geräte, in deren Beschreibung keines der gewählten Tags vorkommt, in das Richtlinienprofil aufgenommen. Wenn diese Option deaktiviert ist, wird das Kriterium nicht angewendet.

  Diese Option ist standardmäßig deaktiviert.

- **Regeln für die Verwendung von Active Directory**

  Aktivieren Sie dieses Kontrollkästchen, um die Aktivierungsregeln für das Richtlinienprofil auf dem Gerät anzupassen. Die Regeln sind davon abhängig, ob das Gerät in einer Active Directory-Organisationseinheit (OU) vorhanden ist oder ob das Gerät (oder dessen Eigentümer) zu einer Active Directory-Sicherheitsgruppe gehört.

  Geben Sie für diese Option im nächsten Schritt Folgendes an:

  - **Zugehörigkeit des Gerätebesitzers zur Sicherheitsgruppe Active Directory**

    Bei aktivierter Option wird das Richtlinienprofil auf dem Gerät aktiviert, wenn dessen Inhaber Mitglied der angegebenen Sicherheitsgruppe ist. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

  - **Zugehörigkeit des Geräts zur Sicherheitsgruppe Active Directory**

    Bei aktivierter Option wird das Richtlinienprofil auf dem Gerät aktiviert. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

  - **Gerätezuordnung in der Active Directory-Organisationseinheit**

    Bei aktivierter Option wird das Richtlinienprofil auf einem Gerät aktiviert, das explizit oder implizit in der angegebenen Active Directory-Organisationseinheit (OU) enthalten ist. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt.

    Diese Option ist standardmäßig deaktiviert.

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 Programme, die auf Geräten untergeordneter Gruppen installiert sind, unterbunden.

Verschlüsselung und Datenschutz

Die Datenverschlüsselung senkt das Risiko eines unbeabsichtigten Informationsverlustes im Falle des Diebstahls oder Verlustes Ihres Laptops oder Ihrer Festplatte, sowie beim Zugriff nicht autorisierter Benutzer und Programme auf Daten.

Die folgenden Kaspersky-Programme 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.

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 Security Center Cloud Console 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 für Mac in Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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:

Wechseln 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 **Zeilen in CSV-Datei exportieren** oder auf **Zeilen in TXT-Datei exportieren**.

Liste der Verschlüsselungsereignisse anzeigen

Bei der Ausführung der Aufgaben zur Datenverschlüsselung oder -entschlüsselung auf den Client-Geräten sendet Kaspersky Endpoint Security für Windows an Kaspersky Security Center Cloud Console Informationen über aufgetretene Ereignisse folgender Typen:

- Aufgrund unzureichenden Speicherplatzes kann eine Datei nicht verschlüsselt oder entschlüsselt werden oder ein verschlüsseltes Archiv nicht erstellt werden.
- Aufgrund eines Lizenzproblems kann eine Datei nicht verschlüsselt oder entschlüsselt werden oder ein verschlüsseltes Archiv nicht erstellt werden.

- Aufgrund fehlender Zugriffsrechte kann eine Datei nicht verschlüsselt oder entschlüsselt werden oder ein verschlüsseltes Archiv nicht erstellt werden.
- Das Zugreifen eines Programms auf eine verschlüsselte Datei wurde verweigert.
- Unbekannte Fehler.

Um sich eine Liste der Ereignisse anzeigen zu lassen, die bei einer Datenverschlüsselung auf Geräten aufgetreten sind, gehen Sie wie folgt vor:

Wechseln Sie im Hauptmenü zu **Vorgänge** → **Verschlüsselung und Datenschutz** → **Verschlüsselungsereignisse**.

Wenn sich der Abschnitt nicht im Menü befindet, bedeutet dies, dass er ausgeblendet ist. Aktivieren Sie in den Einstellungen der Benutzeroberfläche die Option **Verschlüsselung und Datenschutz anzeigen**, um den Abschnitt anzuzeigen.

Sie können die Liste der verschlüsselten Laufwerke als csv- oder txt-Datei exportieren. Klicken Sie dazu entweder auf **Zeilen in CSV-Datei exportieren** oder auf **Zeilen in TXT-Datei exportieren**.

Alternativ können Sie die Liste der Verschlüsselungsereignisse für jedes verwaltete Gerät überprüfen.

So zeigen Sie die Verschlüsselungsereignisse eines verwalteten Geräts an:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte**.
2. Klicken Sie auf den Namen eines verwalteten Geräts.
3. Wechseln Sie auf der Registerkarte **Allgemein** zum Abschnitt **Schutz**.
4. Klicken Sie auf den Link **Fehler der Datenverschlüsselung anzeigen**.

Verschlüsselungsberichte erstellen und anzeigen

Sie können folgende Berichte erstellen:

- Bericht über den Verschlüsselungsstatus verwalteter Geräte. Dieser Bericht enthält Details zur Datenverschlüsselung verschiedener verwalteter Geräte. Der Bericht zeigt beispielsweise die Anzahl der Geräte, für welche die Richtlinie mit konfigurierten Verschlüsselungsregeln gilt. Außerdem können Sie ihm entnehmen, wie viele Geräte neu gestartet werden müssen. Darüber hinaus enthält der Bericht Informationen über die Verschlüsselungstechnologie und den Algorithmus für jedes Gerät.
- Bericht über den Verschlüsselungsstatus der Massenspeichergeräte. Dieser Bericht enthält ähnliche Informationen wie der Bericht zum Verschlüsselungsstatus verwalteter Geräte, verfügt aber lediglich über Informationen zu Massenspeichergeräten und Wechseldatenträgern.
- Bericht über Berechtigungen für den Zugriff 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 Programmen auf verschlüsselte Dateien. Dieser Bericht ist hilfreich, wenn nicht autorisierte Benutzer oder Programme versuchen, auf verschlüsselte Dateien oder Laufwerke zuzugreifen.

Im Abschnitt **Überwachung und Berichterstattung** → **Berichte** können Sie jeden Bericht generieren. Alternativ können Sie im Abschnitt **Vorgänge** → **Verschlüsselung und Datenschutz** die folgenden Verschlüsselungsberichte generieren:

- Bericht über den Verschlüsselungsstatus der Massenspeichergeräte
- Bericht über Berechtigungen für den Zugriff 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 einen der folgenden Abschnitte:
   - **Verschlüsselte Laufwerke**, erstellt den Bericht über den Verschlüsselungsstatus der Massenspeichergeräte oder den Bericht über Zugriffsrechte auf verschlüsselte Laufwerke.
   - **Verschlüsselungsereignisse** erstellt den Bericht über Fehler bei der Dateiverschlüsselung.
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 dem Kaspersky-Programm entspricht, mit dem das ausgewählte Laufwerk verschlüsselt wurde.

   Wenn ein Laufwerk mit einem Kaspersky-Programm verschlüsselt ist, das von Kaspersky Security Center Cloud Console nicht unterstützt wird, verwenden Sie die auf der Microsoft Management Console basierende Verwaltungskonsole, um den autonomen Zugriff zu gewähren.

6. Folgen Sie den Anweisungen in der Hilfe von Kaspersky Endpoint Security für Windows (siehe erweiterbare Blöcke am Ende des Abschnitts).

Anschließend kann der Benutzer die empfangene Datei verwenden, um auf das verschlüsselte Laufwerk zuzugreifen und die auf dem Laufwerk gespeicherten Daten zu lesen.

Benutzer und Benutzerrollen

In diesem Abschnitt werden Benutzer und Benutzerrollen beschrieben und Anweisungen zum Erstellen und Ändern dieser Regeln, zum Zuweisen von Rollen und Gruppen zu Benutzern sowie zum Zuordnen von Richtlinienprofilen zu Rollen zur Verfügung gestellt.

Über Benutzerkonten

In Kaspersky Security Center Cloud Console können Benutzerkonten und Gruppen von Benutzerkonten verwaltet werden. Das Programm unterstützt zwei Typen von Benutzerkonten:

- Benutzerkonten der Mitarbeiter einer Organisation. Der Administrationsserver erhält Daten über die Konten dieser lokalen Benutzer beim Abfragen des Unternehmensnetzwerks.
- Benutzerkonten für interne Benutzer von Kaspersky Security Center Cloud Console. Auf dem Portal können Sie Konten von internen Benutzern erstellen. Diese Benutzerkonten werden nur in Kaspersky Security Center Cloud Console verwendet.

So zeigen Sie Tabellen mit Benutzerkonten und Benutzergruppen an:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen**.
2. Wählen Sie die Registerkarte **Benutzer** oder **Gruppen** aus.

Die Tabelle der Benutzer oder Benutzergruppen wird geöffnet. Standardmäßig wird die geöffnete Tabelle nach den Spalten **Untertyp** 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 **Untertyp** auf **Lokal**.

Wenn Sie auf einen sekundären Administrationsserver wechseln, der älter als einschließlich Version 14.2 ist, und anschließend die Liste der Benutzer oder Benutzergruppen öffnen, wird die geöffnete Tabelle nur nach der Spalte **Untertyp** gefiltert. Der Filter nach der Spalte **Zugeordnete Rollen** wird standardmäßig nicht angewendet. Die gefilterte Tabelle enthält alle internen Benutzer oder Benutzergruppen mit und ohne der zugewiesenen Rolle.

Hinzufügen eines Benutzerkontos eines internen Benutzers

Bei Bedarf können Sie auf dem Portal interne Benutzer aus Ihrem Arbeitsbereich hinzufügen. Nachdem Sie einen internen Benutzer hinzugefügt haben, können Sie ihm in Kaspersky Security Center Cloud Console eine Rolle zuweisen.

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 Anwendung von Kaspersky 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 Security Center Cloud Console bietet Unterstützungen für eine rollenbasierte Zugriffskontrolle auf die Funktionen von Kaspersky Security Center Cloud Console und von verwalteten Kaspersky-Programmen an.

Sie können die Zugriffsrechte auf Programmfunktionen für Benutzer von Kaspersky Security Center Cloud Console mit einer der folgenden Methoden konfigurieren:

- Durch individuelle Konfiguration der Berechtigungen jedes Benutzers bzw. jeder Benutzergruppe.
- Durch Erstellen typischer Benutzerrollen mit einer vordefinierten Auswahl von Berechtigungen und Zuweisung der Rollen an die Benutzer entsprechend ihrer dienstlichen Verpflichtungen.

Die Verwendung von Benutzerrollen soll die stets wiederkehrenden Abläufe für das Konfigurieren von Zugriffsrechten der Benutzer auf Programmfunktionen vereinfachen und verkürzen. Die Zugriffsberechtigungen werden in der Rolle entsprechend der typischen Aufgaben und dienstlichen Verpflichtungen des Benutzers festgelegt.

Die Benutzerrollen können einen ihrem Verwendungszweck entsprechenden Namen erhalten. Es kann eine unbegrenzte Anzahl von Rollen erstellt werden.

Sie können entweder vorkonfigurierte 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 Security Center Cloud Console 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**.

Zugriffsrechte auf Programmfunktionen

Funktionsbereich	Berechtigung	Benutzervorgang: Benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe
Allgemeine Funktionen: **Verwaltung von Administrationsgruppen**	**Schreiben**	• Hinzufügen eines Geräts zu einer Administrationsgruppe: **Schreiben**	Nichts

		• Löschen eines Geräts aus einer Administrationsgruppe: **Schreiben** • Hinzufügen einer Administrationsgruppe zu einer anderen Administrationsgruppe: **Schreiben** • Löschen einer Administrationsgruppe aus einer anderen Administrationsgruppe: **Schreiben**	
Allgemeine Funktionen: **Zugriff auf Objekte, unabhängig von ihren ACLs**	**Lesen**	Lesenden Zugriff auf alle Objekte bekommen: **Lesen**	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 U in die Datenverw des Administrationss • "Berichte sende • "Installationspak verteilen" • "Remote-Installa eines Programm sekundären Administrationss

Allgemeine Funktionen: **Gelöschte Objekte**	• **Lesen**	• Gelöschte Objekte im	Nichts

	• **Schreiben**	Papierkorb anzeigen: **Lesen** • Objekte aus dem Papierkorb löschen: **Schreiben**	
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
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
Allgemeine Funktionen:	• **Schlüsseldatei**	• Schlüsseldatei	Nichts

Verwaltung von Lizenzschlüsseln	**exportieren** • **Schreiben**	exportieren: **Schlüsseldatei exportieren** • Einstellungen des Lizenzschlüssels des Administrationsservers ändern: **Schreiben**	
Allgemeine Funktionen: **Erzwungene Berichtsverwaltung**	• **Lesen** • **Schreiben**	• Berichte unabhängig von ihren ACLs erstellen: **Schreiben** • Berichte unabhängig von ihren ACLs exportieren: **Lesen**	Nichts
Allgemeine Funktionen: **Hierarchie von Administrationsservern**	**Hierarchie von Administrationsservern konfigurieren**	Sekundäre Administrationsserver registrieren, aktualisieren oder löschen: **Hierarchie von Administrationsservern konfigurieren**	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
Allgemeine Funktionen: **Virtuelle Administrationsserver**	• **Virtuelle Administrationsserver verwalten** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen**	• Liste mit virtuellen Administrationsservern abrufen: **Lesen** • Informationen über den virtuellen Administrationsserver erhalten: **Lesen** • Virtuellen Administrationsserver erstellen, aktualisieren	Nichts

	ausführen	oder löschen: **Virtuelle Administrationsserver verwalten** • Virtuellen Administrationsserver in andere Gruppe verschieben: **Virtuelle Administrationsserver verwalten** • Rechte des virtuellen Administrationsservers angeben: **Virtuelle Administrationsserver verwalten**	
Allgemeine Funktionen: Verwaltung der Chiffrierschlüssel	**Schreiben**	Importieren von Chiffrierschlüsseln: **Schreiben**	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
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
Systemverwaltung: Network Access Control	• **Lesen** • **Schreiben**	• CISCO-Einstellungen anzeigen: **Lesen**	Nichts

		• CISCO-Einstellungen ändern: **Schreiben**	
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 a Basis eines Referenzimages vo Betriebssystem ers
Systemverwaltung: **Schwachstellen- und Patch-Management**	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	• Eigenschaften von Patches von Drittherstellern anzeigen: **Lesen** • Eigenschaften von Patches von Drittherstellern ändern: **Schreiben**	• "Synchronisatio Windows Updat durchführen" • "Updates von W Update installier • "Schwachsteller schließen" • "Erforderliche U installieren und Schwachstellen schließen"
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
Systemverwaltung: **Software-Inventur**	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen**	Nichts	Nichts

	ausführen		

Vorkonfigurierte Benutzerrollen

Benutzerrollen, die Benutzern von Kaspersky Security Center Cloud Console zugewiesen werden, gewähren Zugriffsrechte für Programmfunktionen.

Sie können entweder vorkonfigurierte Benutzerrollen mit bereits festgelegten Zugriffsrechten verwenden oder neue Rollen erstellen und die notwendigen Berechtigungen selbst konfigurieren. Einige der in Kaspersky Security Center Cloud Console verfügbaren, vorkonfigurierten Rollen können entsprechenden beruflichen Positionen, wie bspw. **Auditor**, **Security Officer** oder **Supervisor** zugeordnet werden (Diese Rollen stehen in Kaspersky Security Center Cloud Console 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 Vorgänge mit allen Berichtstypen, alle Anzeige-Vorgänge, einschließlich der Anzeige gelöschter Objekte (gewährt die Berechtigungen **Lesen** und **Schreiben** im Bereich **Gelöschte Objekte**). Erlaubt keine anderen Vorgänge. Sie können diese Rolle einer Person zuweisen, die das Audit Ihres Unternehmens durchführt.
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**.

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** • **Kaspersky Softwareverteilung** • **Virtuelle Administrationsserver** • **Verwaltung mobiler Geräte: Allgemein** • **Systemverwaltung**, inklusive aller Funktionen • Alle Funktionen aus dem Bereich von Kaspersky Endpoint Security
Administrator der Funktion "Verwaltung mobiler Geräte"	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen: • **Allgemeine Funktionen: Grundlegende Funktionen** • **Verwaltung mobiler Geräte: Allgemein**
Operator der Funktion "Verwaltung mobiler Geräte"	Gewährt die Berechtigungen **Lesen** und **Ausführen** in dem Funktionsbereich **Allgemeine Funktionen**: **Grundlegende Funktionen**. Gewährt die Berechtigungen **Lesen** und **Nur Informationsbefehle an mobile Geräte senden** in den Funktionsbereichen **Verwaltung mobiler Geräte**: **Allgemein**.
Security Officer	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen in **Allgemeine Funktionen**: • **Zugriff auf Objekte, unabhängig von deren ACLs** • **Erzwungene Berichtsverwaltung** Gewährt die Berechtigungen **Lesen**, **Schreiben**, **Ausführen**, **Dateien von Geräten auf dem Administrator-Arbeitsplatz speichern** und **Ausführen von Vorgängen für die Geräteauswahlen** im Funktionsbereich **Systemverwaltung: Verbindungen**. Sie können diese Rolle einem Beauftragten zuweisen, der für die IT-Sicherheit in Ihrer Organisation zuständig ist.
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. Wechseln Sie je nach Objekttyp im Hauptmenü zum entsprechenden Abschnitt:
   - **Geräte → Gruppenhierarchie**
   - **Geräte → Aufgaben**
   - **Überwachung und Berichterstattung → Berichte**
   - **Geräte → Geräteauswahlen**
   - **Überwachung und Berichterstattung → Ereignisauswahlen**
2. Öffnen Sie die Eigenschaften des Objekts, für das Sie Zugriffsrechte konfigurieren möchten.

   Um das Eigenschaftsfenster einer Administrationsgruppe oder einer Aufgabe zu öffnen, klicken Sie auf den Objektnamen. Eigenschaften anderer Objekte können über die Schaltfläche in der Werkzeugleiste geöffnet werden.
3. Wechseln 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.

Benutzern oder Benutzergruppen eine Rolle zuweisen

So weisen Sie einem Benutzer oder einer Benutzergruppe 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 Benutzergruppe aus, dem oder der Sie die Rolle zuweisen wollen.

   Es können mehrere Namen ausgewählt werden.
3. Klicken Sie in der Menüleiste auf die Schaltfläche **Rolle zuordnen**.

   Der Assistent zum Zuweisen einer Rolle wird gestartet.
4. Folgen Sie den Anweisungen des Assistenten: Wählen Sie die Rolle aus, die Sie den ausgewählten Benutzern oder Benutzergruppen 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, deb Benutzern oder der Benutzergruppe die Rolle mit einer Auswahl von Berechtigungen für die Arbeit mit dem Administrationsserver zugewiesen. In der Liste der Benutzer wird in der Spalte **Zugeordnete Rollen** ein Kontrollkästchen angezeigt.

Erstellen einer Benutzerrolle

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 Programme von Kaspersky.
6. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die neue Rolle wird in der Liste der Benutzerrollen angezeigt.

Zugriffsrechte eines Benutzers bearbeiten

Für die folgenden Objekte können Sie Benutzerzugriffsrechte bearbeiten:

- Administrationsserver
- Administrationsgruppe
- Aufgabe
- Bericht
- Ereignisauswahl
- Geräteauswahl

So bearbeiten Sie die Zugriffsrechte für einen Benutzer:

1. Wechseln Sie zur Registerkarte **Zugriffsrechte** des ausgewählten Objekts.
2. Wählen Sie einen Benutzer aus, für den Sie Zugriffsrechte bearbeiten möchten.

   Wenn Sie Ihr eigenes Benutzerkonto ausgewählt haben, können Sie Ihre eigenen Zugriffsrechte nicht widerrufen. Die Änderungen werden nicht übernommen.
3. Klicken Sie auf die Schaltfläche **Zugriffsrechte**.
4. Bearbeiten Sie im sich öffnenden Fenster die Zugriffsrechte für den ausgewählten Benutzer.
5. Klicken Sie auf die Schaltfläche **OK**.

Die Zugriffsrechte wurden für diesen Benutzer geändert.

Bearbeiten einer Benutzerrolle

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 Programme von Kaspersky.
4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die aktualisierte Rolle wird in der Liste der Benutzerrollen angezeigt.

Bearbeiten des Bereichs einer Benutzerrolle

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 auf der Seite **Rolle auswählen** des Assistenten die Benutzerrolle aus, die Sie zuweisen möchten.
5. Wählen Sie auf der Seite **Bereich definieren** des Assistenten 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. Wechseln 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 auf der Seite **Bereich definieren** des Assistenten die Administrationsgruppe aus, die Sie dem Gültigkeitsbereich der Benutzerrolle hinzufügen möchten.
6. Wählen Sie auf der Seite **Benutzer auswählen** des Assistenten 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.

Löschen einer Benutzerrolle

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.

Verbinden von Richtlinienprofilen mit Rollen

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. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Rollen**.
2. Klicken Sie auf den Namen und die Rolle, die Sie mit einem Richtlinienprofil verbinden möchten.

   Das Fenster "Rolleneigenschaften" wird geöffnet, in dem die Registerkarte **Allgemein** ausgewählt ist.
3. Wählen Sie die Registerkarte **Einstellungen** aus und scrollen Sie nach unten zum Abschnitt **Richtlinien und Profile**.
4. Klicken Sie auf die Schaltfläche **Bearbeiten**.
5. Um die Rolle mit einem der folgenden Profile zu verbinden, gehen Sie wie folgt vor:

   - **Vorhandenes Richtlinienprofil**: Klicken Sie auf den Richtungspfeil (>) 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.

Erstellen einer Benutzergruppe

So erstellen Sie eine Benutzergruppe:

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 Benutzergruppe an:

   - **Name**
   - **Beschreibung**

4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

Eine neue Benutzergruppe wird zur Liste mit Benutzergruppen hinzugefügt.

Bearbeiten einer Benutzergruppe

So bearbeiten Sie eine Benutzergruppe:

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 Gruppe, die Sie bearbeiten möchten.
3. Ändern Sie im folgenden Fenster für Gruppeneinstellungen die Einstellungen für die Benutzergruppe:

   - Auf der Registerkarte **Allgemein** können Sie die Einstellungen **Name** und **Beschreibung** ändern. Diese Einstellungen sind nur für interne Benutzergruppen verfügbar.
   - Auf der Registerkarte **Benutzer** können Sie Benutzer zur Benutzergruppe hinzufügen. Diese Einstellung ist nur für interne Benutzer und interne Benutzergruppen verfügbar.
   - Auf der Registerkarte **Rollen** können Sie einer Benutzergruppe eine Rolle zuweisen.

4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die Änderungen werden auf die Benutzergruppe angewendet.

Hinzufügen von Benutzerkonten zu einer internen Gruppe

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 Benutzergruppe

Sie können nur interne Benutzergruppen 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 Security Center Cloud Console anmelden können, müssen Sie die Integration mit Active Directory Federation Services (ADFS) konfigurieren.

Kaspersky Security Center Cloud Console unterstützt ADFS 3 (Windows Server 2016) oder eine neuere Version.

Um die Einstellungen der ADFS-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 ADFS-Integration:

1. Klicken Sie im Hauptmenü auf das Einstellungen-Symbol ( ) neben dem Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Integrationseinstellungen von ADFS** aus.
3. Kopieren Sie die Callback-URL.

   Sie benötigen diese URL, um die Integration in der ADFS-Verwaltungskonsole zu konfigurieren.

4. Fügen Sie in der ADFS-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 ADFS-Verwaltungskonsole generiert eine Client-ID für die neue Anwendung. Sie benötigen die Client-ID, um die Integration in Kaspersky Security Center Cloud Console zu konfigurieren.

5. Geben Sie als Redirect-URI die Callback-URL an, die Sie im Eigenschaftenfenster des Administrationsservers kopiert haben.

6. Generieren Sie ein Clientgeheimnis. Sie benötigen das Clientgeheimnis, um die Integration in Kaspersky Security Center Cloud Console 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 Security Center Cloud Console den Abschnitt **Integrationseinstellungen von ADFS** erneut.

14. Stellen Sie den Umschalter auf die Position **ADFS-Integration 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 von ADFS** 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 Security Center Cloud Console 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 Security Center Cloud Console zu identifizieren. Die Client-ID finden Sie in der ADFS-Verwaltungskonsole im Eigenschaftenfenster der Serveranwendung, die der Kaspersky Security Center Cloud Console entspricht.

- **Client-Geheimnis**

  Das Clientgeheimnis generieren Sie in der ADFS-Verwaltungskonsole, wenn Sie die Eigenschaften der Serveranwendung angeben, die der Kaspersky Security Center Cloud Console entspricht.

- **Domäne, deren Benutzer authentifiziert werden sollen**

  Die Mitglieder der ausgewählten Domäne können sich mit ihren Zugangsdaten für das Domänenkonto an der Kaspersky Security Center Cloud Console anmelden. Die Domänennamen werden in der Liste angezeigt, nachdem Sie die Netzwerkabfrage abgeschlossen haben.

- **Feldname der Benutzer-SID in dem ID-Token**

  Name des Felds, das auf die Benutzer-SID im ID-Token verweist. Der Feldname wird benötigt, um den Benutzer an der Kaspersky Security Center Cloud Console zu identifizieren. Standardmäßig heißt dieses Feld im ID-Token "primarysid".

- **Feldname des Arrays mit Benutzergruppen-SIDs in dem 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. Klicken Sie auf die Schaltfläche **Speichern**.

Die Integration mit ADFS ist abgeschlossen. Um sich mit den Zugangsdaten eines AD-Kontos an der Kaspersky Security Center Cloud Console anzumelden, verwenden Sie den Link aus dem Abschnitt **Integrationseinstellungen von ADFS** (**Link zur ADFS-Anmeldung an Kaspersky Security Center Cloud Console**).

Wenn Sie sich zum ersten Mal mittels ADFS an der Kaspersky Security Center Cloud Console anmelden, reagiert die Konsole möglicherweise mit einer Verzögerung.

Einen Benutzer zum Gerätebesitzer machen

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 **Geräte** → **Verwaltete Geräte** ausgeführt werden: Klicken Sie auf den Namen des Geräts, das Sie zuweisen möchten, und klicken Sie dann auf den Link **Gerätebesitzer verwalten**.

Arbeit mit den Revisionen der Objekte

Der Abschnitt enthält Informationen über die Arbeit mit den Revisionen des Objekts.

Folgende Objekte unterstützen die Arbeit mit Revisionen:

- Administrationsserver
- Richtlinien
- Aufgaben
- Administrationsgruppen
- Benutzerkonten
- Installationspakete

Über Revisionen von Objekten

Kaspersky Security Center Cloud Console 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.

Sie können mit den Revisionen von Objekten folgende Aktionen ausführen:

- Ausgewählte Revision anzeigen
- Rollback der Änderungen des Objektes auf die ausgewählte Revision durchführen

Im Eigenschaftenfenster der Objekte, die Revisionen unterstützen, wird im Abschnitt **Revisionsverlauf** eine Liste der Objektrevisionen mit den folgenden Informationen angezeigt:

- Nummer der Revision des Objekts
- Datum und Uhrzeit der Objektänderung
- Name des Benutzers, der das Objekt geändert hat
- Ausgeführte Aktion mit dem Objekt
- Beschreibung der Revision der Änderungen der Objekteinstellungen

  Standardmäßig ist die Beschreibung der Revision des Objekts nicht ausgefüllt. Um eine Beschreibung der Revision hinzuzufügen, wählen Sie die gewünschte Revision aus und klicken Sie auf die Schaltfläche **Beschreibung bearbeiten**. Geben Sie im folgenden Fenster einen Text für die Revisionsbeschreibung ein.

Rollback der Änderungen

Falls erforderlich können Sie ein Rollback der Änderungen des Objekts durchführen. Beispielsweise kann es erforderlich sein, die Einstellungen der Richtlinie auf den Zustand eines bestimmten Datums zurückzusetzen.

Um ein Rollback der Änderungen einer Aufgabe durchzuführen, gehen Sie wie folgt vor:

1. Wechseln Sie zum Abschnitt **Revisionsverlauf** des Objekts.
2. Wählen Sie in der Liste mit den Revisionen des Objekts die Nummer der Revision aus, auf deren Stand die Änderungen zurückgesetzt werden sollen.
3. Klicken Sie auf die Schaltfläche **Rollback**.

Es wird ein Rollback auf die ausgewählte Revision durchgeführt. In der Liste der Revisionen des Objektes wird ein Eintrag über die ausgeführte Aktion angezeigt. In der Beschreibung der Revision werden die Informationen über die Nummer der Revision angezeigt, auf die Sie das Objekt zurückgesetzt haben.

Hinzufügen einer Beschreibung der Revision

Sie können eine Beschreibung für die Revision hinzufügen, damit es künftiger einfacher ist, die gewünschte Revision in der Liste zu finden.

Um eine Beschreibung der Revision hinzuzufügen, gehen Sie wie folgt vor:

1. Wechseln Sie zum Abschnitt **Revisionsverlauf** des Objekts.
2. Wählen Sie in der Liste der Revisionen des Objektes die Revision aus, für die eine Beschreibung hinzugefügt werden soll.
3. Klicken Sie auf die Schaltfläche **Beschreibung bearbeiten**.
4. Geben Sie im folgenden Fenster einen Text für die Revisionsbeschreibung ein.

   Standardmäßig ist die Beschreibung der Revision des Objekts nicht ausgefüllt.
5. Klicken Sie auf die Schaltfläche **Speichern**.

Die neue Beschreibung wird in der Spalte **Beschreibung** in der Tabelle des Revisionsverlaufs angezeigt.

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 das Programm 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 Security Center Cloud Console verarbeitet die Geräte in der Gruppe "Nicht zugeordnete Geräte" gemäß den folgenden Regeln:

- Wenn Sie für die Geräte Verschiebungsregeln konfiguriert haben und ein Gerät die Kriterien einer Verschiebungsregel erfüllt, wird das Gerät gemäß der Regel automatisch 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 vollständiger Festplattenverschlüsselung verschlüsselt ist. Solche Geräte werden nicht automatisch gelöscht und Sie diese ausschließlich manuell löschen. Wenn Sie ein Gerät löschen wollen, das über ein verschlüsseltes Laufwerk verfügt, entschlüsseln Sie zunächst das Laufwerk und löschen Sie anschließend das Gerät.

  Wenn Sie stattdessen das Gerät mit verschlüsseltem Laufwerk löschen, werden auch die zum Entschlüsseln des Laufwerks erforderlichen Daten gelöscht. In diesem Fall müssen zum Entschlüsseln des Laufwerks folgende Bedingungen erfüllt sein:

  - Das Gerät wird erneut mit dem Administrationsserver verbunden, um die zum Entschlüsseln des Laufwerks erforderlichen Daten wiederherzustellen.

  - Der Gerätebenutzer merkt sich das Kennwort für die Entschlüsselung.

  - Die Sicherheitsanwendung, die zum Verschlüsseln des Laufwerks verwendet wurde, bspw. Kaspersky Endpoint Security für Windows, ist weiterhin auf dem Gerät installiert.

  Wenn das Laufwerk mittels Kaspersky-Festplattenverschlüsselung verschlüsselt wurde, können Sie auch versuchen, die Daten mithilfe des Wiederherstellungs-Tools FDERT wiederherzustellen.

Wenn Sie ein Gerät manuell aus der Gruppe "Nicht zugeordnete Geräte" löschen, entfernt das Programm 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 Security Center Cloud Console 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.

Kaspersky-Datenbanken und -Anwendungen aktualisieren

Dieser Abschnitt beschreibt die Schritte, die Sie für ein regelmäßiges Update durchführen müssen:

- Kaspersky-Datenbanken und Programm-Module
- Installierte Programme von Kaspersky, einschließlich der Komponenten von Kaspersky Security Center Cloud Console und der Sicherheitsanwendungen

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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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-Programmen via Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 **Updates verteilen** 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 Security Center Cloud Console 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 Security Center Cloud Console**

Standardmäßig werden die heruntergeladenen Updates und Patches für den Administrationsagenten und andere Komponenten von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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

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 Security Center Cloud Console, ob die Kaspersky-Server erreichbar sind. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet das Programm öffentliche DNS-Server. Dies ist erforderlich, um sicherzustellen, dass die Antiviren-Datenbanken aktualisiert werden und das Sicherheitsniveau für die verwalteten Geräte beibehalten wird.

- Installierte Programme von Kaspersky, einschließlich der Komponenten von Kaspersky Security Center Cloud Console und der Sicherheitsanwendungen

Abhängig von der Konfiguration Ihres Netzwerks können Sie die folgenden Schemata für das Herunterladen und Verteilen der erforderlichen Updates auf die verwalteten Geräte verwenden:

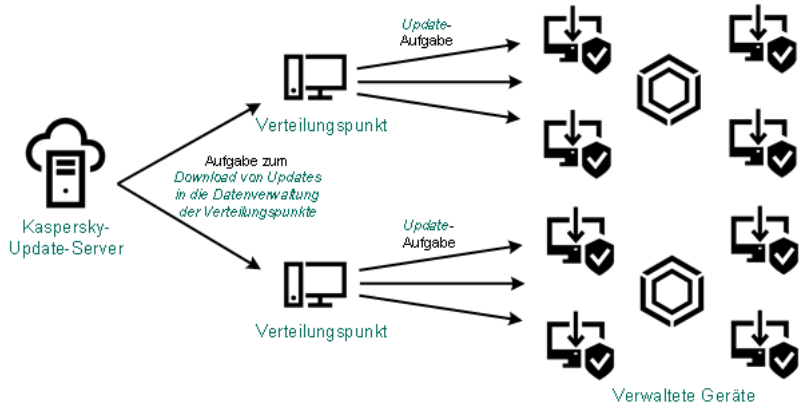
- Verwenden der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*
- Manuell über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server
- Direkt von den Kaspersky Update-Servern zu Sicherheitsanwendungen auf den verwalteten Geräten

Verwenden der Aufgabe Updates in die Datenverwaltung der Verteilungspunkte herunterladen

In diesem Schema lädt Kaspersky Security Center Cloud Console 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 Security Center Cloud Console

  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.

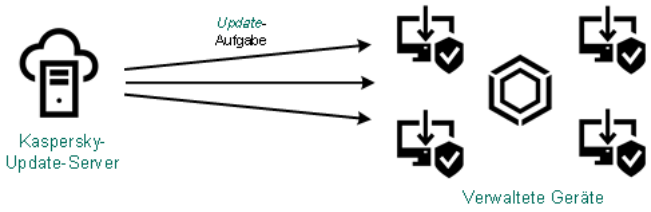
Manuell über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server

Wenn die Client-Geräte keine Verbindung zum Verteilungspunkt haben, können Sie einen lokalen Ordner oder eine freigegebene Ressource als Quelle für das Update von Kaspersky-Datenbanken, -Softwaremodulen und -Anwendungen verwenden. In diesem Schema müssen Sie die erforderlichen Updates aus der Datenverwaltung des Verteilungspunkts auf einen Wechseldatenträger und dann in den lokalen Ordner oder die als Update-Quelle in den Einstellungen von Kaspersky Endpoint Security für Windows angegebene freigegebene Ressource kopieren (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 können Sie Kaspersky Endpoint Security für Windows so konfigurieren, dass Updates direkt von den Updateservern von Kaspersky empfangen werden (siehe Abbildung unten).



Updates von Sicherheitsanwendungen direkt von Kaspersky Update-Servern aus

In diesem Schema verwendet die Sicherheitsanwendung nicht die von Kaspersky Security Center Cloud Console 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.

Erstellen der Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte

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 Security Center Cloud Console-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 **Geräte** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie für Kaspersky Security Center Cloud Console 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 die Schaltfläche **Erstellen**.

   Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.
8. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.

9. Geben Sie auf der Registerkarte **Programmeinstellungen** im Fenster der Aufgabeneigenschaften die folgenden Einstellungen an:

- **Update-Quellen**

  Als Update-Quelle für den Verteilungspunkt können die folgenden Ressourcen verwendet werden:

  - Kaspersky-Update-Server

    HTTP(S)-Server bei Kaspersky, von denen Programme von Kaspersky Updates für Datenbanken und Programm-Module herunterladen.

    Diese Variante ist standardmäßig festgelegt.

  - Primärer Administrationsserver

    Diese Ressource gilt für Aufgaben, die für einen sekundären oder virtuellen Administrationsserver erstellt wurden.

  - Lokaler Ordner oder Netzwerkordner

    Lokaler oder Netzwerkordner, der die neuesten Updates enthält. Ein Netzwerkordner kann ein FTP- oder HTTP-Server oder eine SMB-Freigabe sein. Für Netzwerkordner, die eine Authentifizierung erfordern, wird nur das SMB-Protokoll unterstützt. Bei Auswahl eines lokalen Ordners ist es erforderlich, einen Ordner auf dem Gerät mit dem installierten Administrationsserver anzugeben.

    Ein FTP- oder HTTP-Server oder ein Netzwerkordner, der von einer Update-Quelle verwendet wird, muss eine Ordnerstruktur (mit Updates) enthalten, die der Struktur entspricht, die bei Verwendung der Kaspersky-Update-Server erstellt wurde.

- **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 Security Center Cloud Console 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 einem der folgenden Programme 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:

- **Start nach Zeitplan**

  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 Option ist standardmäßig aktiviert.

  - **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.

    Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit alle sechs Stunden ausgeführt.

  - **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 Security Center Cloud Console 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, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig sind keine Tage des Monats ausgewählt; die Standardstartzeit ist 18:00:00 Uhr.

- **Beim Erkennen eines Virenangriffs**

Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Programmtypen aus, die Virenangriffe überwachen. Es sind folgende Programmtypen verfügbar:

- Antiviren-Programme für Workstations und Dateiserver
- Anti-Virus für Perimeterschutz
- Anti-Virus für E-Mailsysteme

Standardmäßig sind alle Programmtypen ausgewählt.

Sie können abhängig vom Anti-Virus-Programmtyp, der einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Programmtypen, die Sie nicht benötigen.

- **Nach Beenden einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Sie können auswählen, wie die vorherige Aufgabe abgeschlossen werden muss (erfolgreich oder mit Fehler), um den Start der aktuellen Aufgabe auszulösen. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem sie abgeschlossen ist, die *Aufgabe zur Untersuchung auf Viren* ausführen.

- **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 des Programms von Kaspersky 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.

  Ist diese Option deaktiviert, so werden auf den Client-Geräten nur Aufgaben nach Zeitplan ausgeführt, aber für **Manuell**, **Einmal** und **Sofort** werden Aufgaben nur auf jenen Client-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 aktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)**

Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

11. 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-Programmen 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 **Geräte** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie für Administrationsagenten.
3. Wechseln Sie im Eigenschaftenfenster der Richtlinie zur Registerkarte **Programmeinstellungen**.
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 Security Center Cloud Console aktivieren und deaktivieren

Die automatische Installation der Patches für Komponenten von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console bei der lokalen Installation des Administrationsagenten auf dem Gerät zu deaktivieren, gehen Sie wie folgt vor:

1. Starten Sie die lokale Installation des Administrationsagenten auf dem Gerät.
2. Deaktivieren Sie im Schritt **Erweiterte Einstellungen** das Kontrollkästchen **Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren**.
3. Folgen Sie den Anweisungen des Assistenten.

   Auf dem Gerät wird der Administrationsagent mit der deaktivierten automatischen Installation von Updates und Patches für die Komponenten von Kaspersky Security Center Cloud Console installiert. Sie können die automatische Installation später mithilfe einer der Richtlinie aktivieren.

Um die automatische Installation der Patches für Komponenten von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console mithilfe einer Richtlinie des Administrationsagenten zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie für Administrationsagenten.
3. Wählen Sie im Eigenschaftenfenster der Richtlinie die Registerkarte **Programmeinstellungen** 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 Security Center Cloud Console wird auf diesen Geräten aktiviert (deaktiviert).

Automatische Installation von Updates für Kaspersky Endpoint Security für Windows

Sie können das automatische Datenbanken-Update und das Update der Programm-Module von Kaspersky Endpoint Security für Windows auf den Client-Geräten konfigurieren.

Um den Download und die automatische Installation von Updates für Kaspersky Endpoint Security für Windows auf den Geräten zu konfigurieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie für die Anwendung Kaspersky Endpoint Security für Windows als Aufgabenuntertyp **Update**.
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 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 die Schaltfläche **Erstellen**.

   Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.
9. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.
10. Definieren Sie auf der Registerkarte **Programmeinstellungen** 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console installiert.

    Sie können auch die Option **Kritische Updates für Programm-Module automatisch installieren** aktivieren. Wenn Updates für die Programm-Module verfügbar sind, installiert Kaspersky Endpoint Security für Windows alle Updates mit dem Status *Kritisch* automatisch; die restlichen Updates werden installiert, nachdem Sie diese genehmigt haben.

    Wenn für es für das Update von Programm-Modulen erforderlich ist, dass sich der Benutzer mit den Bedingungen des Lizenzvertrags und Datenschutzrichtlinie vertraut macht und diese akzeptiert, werden die Updates installiert, nachdem der Benutzer die Bedingungen des Lizenzvertrags und der Datenschutzrichtlinie akzeptiert hat.

13. Aktivieren Sie das Kontrollkästchen **Updates in Ordner kopieren**, damit das Programm die heruntergeladenen Updates in einen Ordner kopiert, und geben Sie den Pfad an.

14. Planen Sie die Aufgabe. Um zeitnahe Updates sicher zu stellen, wird empfohlen, die Option **Nach dem Download von Updates in die Datenverwaltung** auszuwählen.

15. Klicken Sie auf die Schaltfläche **Speichern**.

Beim Ausführen der Aufgabe **Update** sendet das Programm Anfragen an die Kaspersky-Update-Server.

Einige Updates erfordern die Installation aktueller Versionen von Verwaltungs-Plug-ins.

Informationen zum Update-Status

Status ist ein Attribut von Softwareupdates, das angibt, ob ein bestimmtes Software-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 Security Center Cloud Console 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 Security Center Cloud Console

  Standardmäßig werden die heruntergeladenen Updates und Patches für Komponenten von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console versuchen, dieses Update von allen Geräten zu deinstallieren.

Genehmigen und Ablehnen von Software-Updates

Die Einstellungen einer Aufgabe zur Installation von Updates 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.

Um ein oder mehrere Updates zu genehmigen oder abzulehnen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Programme von Kaspersky** → **Nahtlose Updates**.

   Eine Liste verfügbarer Updates wird geöffnet.

   > Für Updates verwalteter Anwendungen muss möglicherweise eine bestimmte Mindestversion von Kaspersky Security Center installiert werden. Wenn diese Version höher ist als Ihre aktuelle Version, werden diese Updates zwar angezeigt, können jedoch nicht genehmigt werden. Außerdem können aus solchen Updates keine Installationspakete erstellt werden, bis Sie Kaspersky Security Center aktualisiert haben. Sie werden aufgefordert, Ihre Kaspersky Security Center-Instanz auf die erforderliche Mindestversion zu aktualisieren.

2. Wählen Sie die Updates aus, die Sie genehmigen oder ablehnen möchten.

3. Klicken Sie auf **Genehmigen**, um die ausgewählten Updates zu genehmigen, oder auf **Ablehnen**, um die ausgewählten Updates abzulehnen.

Als Standard gilt der Wert *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, (falls möglich) deinstalliert. Ferner werden sie in Zukunft nicht auf anderen Geräten installiert.

Einige Updates für die Programme von Kaspersky können nicht deinstalliert werden. Wenn Sie den Status *Abgelehnt* für sie festlegen, wird Kaspersky Security Center Cloud Console 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 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 Updates löschen müssen, können Sie diese lokal manuell löschen.

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 **Geräte** → **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 **Programmeinstellungen** 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.

Update der Kaspersky-Datenbanken und Programm-Module auf autonomen Geräten

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.

Update der Datenbanken von Kaspersky Security für Windows Server

Sie können Kaspersky Security für Windows Server auf verwalteten Geräten installieren und bei Bedarf die Aufgabe zum Echtzeitschutz für Dateien des Programms starten. Allerdings wird das Programm ohne die für seinen ordnungsgemäßen Betrieb notwendigen Datenbanken ausgeliefert. Die Datenbanken werden erst dann auf die verwalteten Geräte verteilt, wenn die Aufgabe *Download von Updates in die Datenverwaltung der Verteilungspunkte* abgeschlossen ist.

Wenn Sie unmittelbar nach der Installation von Kaspersky Security für Windows Server auf einem verwalteten Gerät die Aufgabe zum Echtzeitschutz von Dateien auf diesem Gerät ausführen möchten, stellen Sie sicher, dass die Datenbanken für das Programm heruntergeladen wurden und aktuell sind. Andernfalls kann es passieren, dass die Aufgabe nicht korrekt ausgeführt wird.

So stellen Sie sicher, dass die Datenbanken von Kaspersky Security für Windows Server aktuell sind:

1. Vergewissern Sie sich, dass die Aufgabe zum *Download von Updates in die Datenverwaltung der Verteilungspunkte* auf dem Administrationsserver abgeschlossen wurde.

2. Führen Sie eine der folgenden Aktionen aus:

   - Setzen Sie den Startzeitpunkt in den Einstellungen der Aufgabe zum Echtzeitschutz von Dateien auf *Beim Programmstart* und starten Sie das verwaltete Gerät neu.

   - Setzen Sie Bedarf den Startzeitpunkt in den Einstellungen der Aufgabe zum Echtzeitschutz von Dateien manuell auf einen beliebigen Zeitpunkt.

   Die von Kaspersky Security für Windows Server ausgeführte Aufgabe zum Echtzeitschutz von Dateien ist betriebsbereit.

Verwalten von Programmen von Drittanbietern auf Client-Geräten

In diesem Abschnitt werden die Funktionen von Kaspersky Security Center Cloud Console für die Verwaltung von Programmen von Drittanbietern beschrieben, die auf Client-Geräten installiert sind.

Über Anwendungen von Drittanbietern

Kaspersky Security Center Cloud Console kann Ihnen dabei helfen, auf Client-Geräten installierte Software von Drittanbietern zu aktualisieren und die Schwachstellen in der Software von Drittanbietern zu beheben. Kaspersky Security Center Cloud Console kann Software von Drittanbietern nur von der aktuellen Version auf die neueste Version aktualisieren. Die folgende Liste stellt die Software von Drittanbietern dar, die Sie mit Kaspersky Security Center Cloud Console aktualisieren können:

Die Liste der Software von Drittanbietern kann aktualisiert und um neue Anwendungen erweitert werden. Sie können überprüfen, ob Sie die Software von Drittanbietern (die auf den Geräten der Benutzer installiert ist) mit Kaspersky Security Center Cloud Console aktualisieren können, indem Sie die Liste der verfügbaren Updates in der Kaspersky Security Center Cloud Console anzeigen.

- 7-Zip-Developers: 7-Zip
- Adobe-Systems:
  - Adobe Acrobat DC
  - Adobe Acrobat Reader DC
  - Adobe Acrobat
  - Adobe Reader
  - Adobe Shockwave Player
- AIMPDevTeam: AIMP
- ALTAP: Altap Salamander
- Apache Software Foundation: Apache Tomcat
- Apple:
  - Apple iTunes
  - Apple QuickTime
- Armory Technologies, Inc.: Armory
- Cerulean Studios: Trillian Basic
- Ciphrex Corporation: mSIGNA
- Cisco: Cisco Jabber

- Code Sector: TeraCopy
- Codec Guide:
  - K-Lite Codec Pack Basic
  - K-Lite Codec Pack Full
  - K-Lite Codec Pack Mega
  - K-Lite Codec Pack Standard
- DbVis Software AB: DbVisualizer
- Decho Corp.:
  - Mozy Enterprise
  - Mozy Home
  - Mozy Pro
- Dominik Reichl: KeePass Password Safe
- Don HO don.h@free.fr: Notepad++
- DoubleGIS: 2GIS
- Dropbox, Inc.: Dropbox
- EaseUs: EaseUS Todo Backup Free
- Electrum Technologies GmbH: Electrum
- Enter Srl: Iperius Backup
- Eric Lawrence: Fiddler
- EverNote: EverNote
- Exodus Movement Inc: Exodus
- EZB Systems: UltraISO
- Famatech:
  - Radmin
  - Remote Administrator
- Far Manager: FAR Manager
- FastStone Soft: FastStone Image Viewer
- FileZilla Project: FileZilla

- Firebird Developers: Firebird
- Foxit Corporation:
  - Foxit Reader
  - Foxit Reader Enterprise
- Free Download Manager.ORG: Free Download Manager
- GIMP-Projekt: GIMP
- GlavSoft LLC.: TightVNC
- GNU-Projekt: Gpg4win
- Google:
  - Google Earth
  - Google Chrome
  - Google Chrome Enterprise
  - Google Earth Pro
- Inkscape-Projekt: Inkscape
- IrfanView: IrfanView
- iterate GmbH: Cyberduck
- Logitech: SetPoint
- LogMeIn, Inc.:
  - LogMeIn
  - Hamachi
  - LogMeIn Rescue Technician Console
- Martin Prikryl: WinSCP
- Mozilla Foundation:
  - Mozilla Firefox
  - Mozilla Firefox ESR
  - Mozilla SeaMonkey
  - Mozilla Thunderbird
- New Cloud Technologies Ltd: MyOffice Standard. Home Edition

- OpenOffice.org: OpenOffice
- Open Whisper Systems: Signal
- Opera Software: Opera
- Oracle Corporation:
  - Oracle Java JRE
  - Oracle VirtualBox
- PDF44: PDF24 MSI/EXE
- Piriform:
  - CCleaner
  - Defraggler
  - Recuva
  - Speccy
- Postgresql: PostgreSQL
- RealNetworks: RealPlayer Cloud
- RealVNC:
  - RealVNC Server
  - RealVNC Viewer
- Right Hemisphere Inc.: SAP Visual Enterprise Viewer (Complete/Minimum)
- Simon Tatham: PuTTY
- Skype Technologies: Skype for Windows
- Sober Lemur S.a.s.:
  - PDFsam Basic
  - PDFsam Visual
- Softland: FBackup
- Splashtop Inc.: Splashtop Streamer
- Stefan Haglund, Fredrik Haglund, Florian Schmitz: CDBurnerXP
- Sublime HQ Pty Ltd: Sublime Text
- TeamViewer GmbH:

    - TeamViewer Host
    - TeamViewer
- Telegram Messenger LLP: Telegram Desktop
- The Document Foundation:
    - LibreOffice
    - LibreOffice HelpPack
- The Git Development Community:
    - Git for Windows
    - Git LFS
- The Pidgin developer community: Pidgin
- TortoiseSVN Developers: TortoiseSVN
- VideoLAN: VLC media player
- VMware:
    - VMware Player
    - VMware Workstation
- WinRAR Developers: WinRAR
- WinZip: WinZip
- Wireshark Foundation: Wireshark
- Wrike: Wrike
- Zimbra: Zimbra Desktop

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 Security Center Cloud Console 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 Security Center Cloud Console 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 Software-Updates, die gleichzeitig den Status *Genehmigt* besitzen können	100	Nicht unterstützt	1.000
Maximale Anzahl an Software-Updates, die einer Aufgabe manuell hinzugefügt werden können	500	1.000	1.000
Maximale Anzahl an Schwachstellen in Programmen, die einer Aufgabe manuell hinzugefügt werden können	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 Security Center Cloud Console 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 Microsoft-Software auf verwalteten Windows-Geräten Erstellen der Aufgabe *Schwachstellen schließen*	✓	✓	–
Manuelle Installation von Updates in Microsoft-Software auf verwalteten Windows-Geräten Installation von Software-Updates von Drittanbietern mittels der Aufgabe *Windows-Updates installieren*	–	✓	✓
Automatisches, regelbasiertes Installieren von Software-Updates von Drittanbietern und Schließen von Schwachstellen in Programmen von Drittanbietern Erstellen der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* und Installation von Updates Hinzufügen einer Regel für die Installation von Updates	✓	–	✓

Installieren von Software-Updates von Drittanbietern

In diesem Abschnitt werden die Funktionen von Kaspersky Security Center Cloud Console für die Installation von Updates für Programme von Drittanbietern beschrieben, die auf Client-Geräten installiert sind.

Szenario: Aktualisieren von Software von Drittanbietern

Dieser Abschnitt enthält ein Szenario für das Update von Drittanbieter-Software, die auf den Client-Geräten installiert ist. Als Drittanbieter-Software gelten Anwendungen von Microsoft und von anderen Softwareherstellern. Updates für Microsoft-Programme werden vom Dienst "Windows Update" bereitgestellt.

Schritte

Das Aktualisieren von Software von Drittanbietern erfolgt in mehreren Phasen:

1. **Suchen nach erforderlichen Updates**

Führen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* aus, um die für die verwalteten Geräte erforderlichen Software-Updates von Drittanbietern zu suchen. Nach Abschluss dieser Aufgabe erhält Kaspersky Security Center Cloud Console 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 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 Software-Updates von Drittanbietern

3. **Konfigurieren der Installation von Updates**

   Wenn Kaspersky Security Center Cloud Console die Liste der Software-Updates von Drittanbietern 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 Produkte 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 Security Center Cloud Console verwenden, und von dem Modus, in dem Kaspersky Security Center Cloud Console 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 Drittanbieter-Software-Updates

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

Über Software-Updates von Drittanbietern

Mit Kaspersky Security Center Cloud Console können Sie die Updates für Drittanbieter-Software verwalten, die auf verwalteten Geräten installiert ist, und Schwachstellen in Programmen von Microsoft und anderen Herstellern durch die Installation erforderlicher Updates beheben.

Kaspersky Security Center Cloud Console 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 Security Center Cloud 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 Software-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 Prüfung von Dateien verwendet und umfassen die Untersuchung auf Viren, die statische und die dynamische Analyse, die Verhaltensanalyse in der Sandbox-Umgebung, sowie Machine Learning.

Kaspersky-Experten führen keine manuelle Analyse von Software-Updates von Drittanbietern durch, die mit der Funktion "Schwachstellen- und Patch-Management" installiert werden können. Darüber hinaus suchen Kaspersky-Experten weder nach Schwachstellen (bekannt und unbekannt) oder nicht dokumentierten Funktionen in derartigen Updates, noch führen sie an ihnen zusätzliche Analysen, neben denen, die im obigen Abschnitt genannt wurden, durch.

Aufgabe zur Installation von Drittanbieter-Software-Updates

Wenn Metadaten von den Software-Updates von Drittanbietern in die Datenverwaltung heruntergeladen wurden, können Sie die folgenden Aufgaben verwenden, um die Updates auf Client-Geräten zu installieren:

- Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen*

  Diese Aufgabe dient dazu, Updates für Microsoft-Programme zu installieren, einschließlich der Updates, die vom Windows-Update-Dienst angeboten werden, sowie Updates für die Produkte 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 Security Center Cloud Console, 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 Security Center Cloud Console verwenden, und von dem Modus, in dem Kaspersky Security Center Cloud Console arbeitet.

Installieren von Software-Updates von Drittanbietern

Sie können Software-Updates von Drittanbietern 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 Updates von Produkten anderer 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 Security Center Cloud Console verwenden, und von dem Modus, in dem Kaspersky Security Center Cloud Console 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 existierenden Aufgabe hinzufügen.

- Indem Sie den Assistenten zur Installation von Updates ausführen.

  Die Verfügbarkeit des Assistenten zur Installation von Updates hängt von dem Modus der Kaspersky Security Center Cloud Console 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 Software-Updates von Drittanbietern 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 **Geräte** → **Verwaltete Geräte** → **<Gerätename>** → **Erweitert** → **Verfügbare Updates**.
   - Um die Liste mit Updates für ein bestimmtes Programm zu öffnen, wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry** → **<Programmname>** → **Verfügbare Updates**.

   Eine Liste verfügbarer Updates wird geöffnet.

2. Aktivieren Sie die Kontrollkästchen neben den Updates, die Sie installieren möchten.

3. Klicken Sie auf die Schaltfläche **Updates installieren**.

   Zum Installieren bestimmter Software-Updates müssen Sie den Endbenutzer-Lizenzvertrag (EULA) akzeptieren. Wenn Sie die EULA ablehnen, wird das 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 Security Center Cloud Console 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 **Geräte** → **Aufgaben** angezeigt. Wenn Sie sich entschieden haben, die Aufgaben zu einer existierenden Aufgabe hinzuzufügen, werden die Updates in den Aufgabeneigenschaften gespeichert.

Um Software-Updates von Drittanbietern 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 zur Installation von Updates

Die Verfügbarkeit dieser Funktion hängt vom Modus der Kaspersky Security Center Cloud Console und Ihrer aktuellen Lizenz ab.

Um eine Aufgabe zur Installation der Software-Updates von Drittanbietern mithilfe des Assistenten zur 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 die Schaltfläche **Assistent zur Installation von Updates starten**.

   Der Assistent zur Installation von Updates wird gestartet. Die Seite **Wählen Sie die Aufgabe zur Installation von Updates aus** zeigt Ihnen die Liste aller existierenden 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 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 von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Schweregrad des ausgewählten Updates (**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 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 Security Center Cloud Console installiert nur die Updates, die sich auf Programme beziehen, die vom selben Anbieter wie das ausgewählte Update erstellt wurden. Abgelehnte Updates und Updates für Programme anderer Anbieter werden nicht installiert.

Diese Option ist standardmäßig deaktiviert.

- **Regel für die Installation von Updates vom Typ**
- **Regel für die Installation des ausgewählten Updates**
- **Ausgewählte Updates bestätigen**

  Das ausgewählte Update wird zur Installation freigegeben. Aktivieren Sie diese Option, wenn einige übernommene Regeln zur Installation von Updates nur die Installation von bestätigten Updates erlauben.

  Diese Option ist standardmäßig deaktiviert.

- **Alle vorherigen Programm-Updates, die für die Installation der ausgewählten Updates erforderlich sind, automatisch installieren**

  Lassen Sie diese Option optimiert, wenn Sie mit der Installation von Programmzwischenversionen einverstanden sind, wenn 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 eine geradlinige Weist 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.

  Wenn Sie beispielsweise Version 3 eines Programms auf einem Gerät installiert haben und Sie es auf Version 5 aktualisieren möchten, Version 5 dieses Programms aber nur über Version 4 installiert werden kann. 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 die Schaltfläche **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 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 von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Schweregrad des ausgewählten Updates (**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 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 Security Center Cloud Console installiert nur die Updates, die sich auf Programme beziehen, die vom selben Anbieter wie das ausgewählte Update erstellt wurden. Abgelehnte Updates und Updates für Programme anderer Anbieter werden nicht installiert.

  Diese Option ist standardmäßig deaktiviert.

- **Regel für die Installation von Updates vom Typ**
- **Regel für die Installation des ausgewählten Updates**
- Ausgewählte Updates bestätigen

  Das ausgewählte Update wird zur Installation freigegeben. Aktivieren Sie diese Option, wenn einige übernommene Regeln zur Installation von Updates nur die Installation von bestätigten Updates erlauben.

  Diese Option ist standardmäßig deaktiviert.

- Alle vorherigen Programm-Updates, die für die Installation der ausgewählten Updates erforderlich sind, automatisch installieren

Lassen Sie diese Option optimiert, wenn Sie mit der Installation von Programmzwischenversionen einverstanden sind, wenn 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 eine geradlinige Weist 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.

Wenn Sie beispielsweise Version 3 eines Programms auf einem Gerät installiert haben und Sie es auf Version 5 aktualisieren möchten, Version 5 dieses Programms aber nur über Version 4 installiert werden kann. 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 existierenden Aufgabe hinzuzufügen, wird das Fenster mit den Aufgabeneigenschaften geöffnet. Die neue Regel wurde den Aufgabeneigenschaften bereits hinzugefügt. Sie können die Regel oder andere Aufgabeneigenschaften anzeigen und anpassen. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Wenn Sie eine Aufgabe erstellen möchten, fahren Sie im Assistenten für das Erstellen einer Aufgabe mit der Erstellung der Aufgabe fort. Die neue Regel, die Sie im Assistenten zur Installation von Updates hinzugefügt haben, wird im Assistenten für das Erstellen einer Aufgabe angezeigt. Wenn Sie den Assistenten 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 Security Center Cloud Console eine Liste der erkannten Schwachstellen und der erforderlichen Updates für die Software von Drittanbietern, die auf den verwalteten Geräten installiert ist.

Die Aufgabe Suche nach Schwachstellen und erforderlichen Updates wird automatisch erstellt, wenn der Schnellstartassistent ausgeführt wird. Wenn Sie den Assistenten nicht ausgeführt haben, erstellen Sie die Aufgabe manuell.

So erstellen Sie die Aufgabe Suche nach Schwachstellen und erforderlichen Updates:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie für Kaspersky Security Center Cloud Console 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 die Schaltfläche **Erstellen**.

   Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.

8. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.

9. Geben Sie im Fenster mit den Aufgabeneigenschaften die allgemeinen Aufgabeneinstellungen an.

10. Geben Sie auf der Registerkarte **Programmeinstellungen** die folgenden Einstellungen an:

    - **Nach Schwachstellen und Updates suchen, die von Microsoft gelistet werden**

      Wenn Kaspersky Security Center Cloud Console 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.

    - **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 Security Center Cloud Console (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 jene Informationen über geeignete Microsoft-Windows-Updates, die zuvor von der Quelle der Microsoft-Updates empfangen wurden und im Geräte-Cache gespeichert sind.

Das Herstellen einer Verbindung zur Update-Quelle von Microsoft kann viele Ressourcen in Anspruch nehmen. 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 festlegen. Wenn Sie diese Option nicht deaktivieren möchten, können Sie den Aufgabenzeitplan so anpassen, dass die Aufgabenstarts innerhalb von 360 Minuten zufällig verzögert werden, um so die Serverüberladung zu reduzieren.

Diese Option ist standardmäßig aktiviert.

Der Modus für den Update-Download beruht auf einer Kombination der folgenden Optionen, mit denen die Einstellungen der Administrationsagenten-Richtlinie festgelegt werden:

- Um Updates abzurufen, stellt der Windows Update-Agent auf einem verwalteten Gerät nur dann eine Verbindung zum Update-Server her, wenn die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** aktiviert ist und die Option **Aktiv** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist.
- Der Windows Update-Agent auf einem verwalteten Gerät verwendet jene Informationen über geeignete Microsoft-Windows-Updates, die zuvor von der Quelle der Microsoft-Updates empfangen wurden und im Geräte-Cache gespeichert sind, sofern die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** aktiviert ist und die Option **Offline** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist, oder wenn die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** deaktiviert ist und die Option **Aktiv** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist.
- Unabhängig vom Status der Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** (aktiviert oder deaktiviert) fordert Kaspersky Security Center Cloud Console keine Informationen über Updates an, wenn die Option **Deaktiviert** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist.

- Nach Schwachstellen und Updates von Drittherstellern suchen, die von Kaspersky gelistet werden

Wenn diese Option aktiviert ist, sucht Kaspersky Security Center Cloud Console in der Windows-Registrierung und den unter Geben Sie Pfade für eine zusätzliche Suche nach Programmen im Dateisystem an **Geben Sie Pfade zur erweiterten Suche von Programmen im Dateisystem an** festgelegten Ordnern nach Schwachstellen und erforderlichen Updates für fremde Produkte (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft entwickelt wurden). Die vollständige Liste von unterstützten Drittanbieter-Apps wird von Kaspersky verwaltet.

Wenn diese Option deaktiviert ist, sucht Kaspersky Security Center Cloud Console nicht nach Schwachstellen und erforderlichen Updates für Drittanbieter-Programme. Sie möchten diese Option beispielsweise deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft Windows-Updates und Updates für Drittanbieter-Apps haben.

Diese Option ist standardmäßig aktiviert.

- **Pfade für die erweiterte Suche nach Anwendungen im Dateisystem angeben**

  Die Ordner, in denen Kaspersky Security Center Cloud Console 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, führt der Administrationsagent die Ablaufverfolgung auch dann durch, wenn die Ablaufverfolgung für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center Cloud Console 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, beginnt der Administrationsagent sie wieder von vorn zu überschreiben. 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 Security Center Cloud Console durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

  Beim Erstellen einer Aufgabe, müssen Sie die erweiterte Diagnose nicht aktivieren. Sie möchten diese Funktion möglicherweise später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen empfangen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Dateien für die erweiterte Diagnose (MB)**

  Der Standardwert beträgt 100 MB und verfügbare Werte liegen zwischen 1 MB und 2048 MB. 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.

Zusätzlich zu den allgemeinen Aufgabeneinstellungen können Sie die folgenden Einstellungen vornehmen, wenn Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* erstellen oder wenn Sie später die Eigenschaften der erstellten Aufgabe anpassen:

- **Nach Schwachstellen und Updates suchen, die von Microsoft gelistet werden**

  Wenn Kaspersky Security Center Cloud Console 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.

- **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 Security Center Cloud Console (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 jene Informationen über geeignete Microsoft-Windows-Updates, die zuvor von der Quelle der Microsoft-Updates empfangen wurden und im Geräte-Cache gespeichert sind.

Das Herstellen einer Verbindung zur Update-Quelle von Microsoft kann viele Ressourcen in Anspruch nehmen. 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 festlegen. Wenn Sie diese Option nicht deaktivieren möchten, können Sie den Aufgabenzeitplan so anpassen, dass die Aufgabenstarts innerhalb von 360 Minuten zufällig verzögert werden, um so die Serverüberladung zu reduzieren.

Diese Option ist standardmäßig aktiviert.

Der Modus für den Update-Download beruht auf einer Kombination der folgenden Optionen, mit denen die Einstellungen der Administrationsagenten-Richtlinie festgelegt werden:

- Um Updates abzurufen, stellt der Windows Update-Agent auf einem verwalteten Gerät nur dann eine Verbindung zum Update-Server her, wenn die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** aktiviert ist und die Option **Aktiv** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist.
- Der Windows Update-Agent auf einem verwalteten Gerät verwendet jene Informationen über geeignete Microsoft-Windows-Updates, die zuvor von der Quelle der Microsoft-Updates empfangen wurden und im Geräte-Cache gespeichert sind, sofern die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** aktiviert ist und die Option **Offline** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist, oder wenn die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** deaktiviert ist und die Option **Aktiv** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist.
- Unabhängig vom Status der Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** (aktiviert oder deaktiviert) fordert Kaspersky Security Center Cloud Console keine Informationen über Updates an, wenn die Option **Deaktiviert** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist.

- Nach Schwachstellen und Updates von Drittherstellern suchen, die von Kaspersky gelistet werden

Wenn diese Option aktiviert ist, sucht Kaspersky Security Center Cloud Console in der Windows-Registrierung und den unter Geben Sie Pfade für eine zusätzliche Suche nach Programmen im Dateisystem an **Geben Sie Pfade zur erweiterten Suche von Programmen im Dateisystem an** festgelegten Ordnern nach Schwachstellen und erforderlichen Updates für fremde Produkte (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft entwickelt wurden). Die vollständige Liste von unterstützten Drittanbieter-Apps wird von Kaspersky verwaltet.

Wenn diese Option deaktiviert ist, sucht Kaspersky Security Center Cloud Console nicht nach Schwachstellen und erforderlichen Updates für Drittanbieter-Programme. Sie möchten diese Option beispielsweise deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft Windows-Updates und Updates für Drittanbieter-Apps haben.

Diese Option ist standardmäßig aktiviert.

- **Pfade für die erweiterte Suche nach Anwendungen im Dateisystem angeben**

  Die Ordner, in denen Kaspersky Security Center Cloud Console 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, führt der Administrationsagent die Ablaufverfolgung auch dann durch, wenn die Ablaufverfolgung für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center Cloud Console 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, beginnt der Administrationsagent sie wieder von vorn zu überschreiben. 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 Security Center Cloud Console durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

  Beim Erstellen einer Aufgabe, müssen Sie die erweiterte Diagnose nicht aktivieren. Sie möchten diese Funktion möglicherweise später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen empfangen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Dateien für die erweiterte Diagnose (MB)**

  Der Standardwert beträgt 100 MB und verfügbare Werte liegen zwischen 1 MB und 2048 MB. 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.

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.

Der Start der Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* ist standardmäßig für 18:00 Uhr geplant. Wenn die Dienstvorschriften des Unternehmens zu diesem Zeitpunkt das Deaktivieren der Geräte vorsehen, 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 des Geräts veranlassen kann. Es ist erforderlich, den optimalen Zeitplan der Aufgabe ausgehend von den im Unternehmen geltenden Dienstvorschriften zu konfigurieren.

Erstellen der Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen"

Die Verfügbarkeit der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* hängt vom Modus der Kaspersky Security Center Cloud Console 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 zur Installation von Updates oder den Assistenten zum 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 Software-Updates haben eine Reihe von Einschränkungen. Diese Einschränkungen sind abhängig von der Lizenz, unter der Sie Kaspersky Security Center Cloud Console verwenden, und von dem Modus, in dem Kaspersky Security Center Cloud Console arbeitet.

So erstellen Sie die Aufgabe Erforderliche Updates installieren und Schwachstellen schließen:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie für Kaspersky Security Center Cloud Console 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**

  Wenn diese Option aktiviert ist, werden Updates installiert, wenn das Gerät neu gestartet oder heruntergefahren wird. Anderenfalls werden Updates gemäß einem Zeitplan installiert.

  Verwenden Sie diese Option, wenn die Installation von Updates die Leistung des Geräts beeinträchtigen könnte.

  Diese Option ist standardmäßig deaktiviert.

- **Erforderliche allgemeine Systemkomponenten installieren**

  Wenn diese Option aktiviert ist, installiert die Anwendung vor der Installation eines Updates automatisch alle allgemeinen Systemkomponenten (erforderlichen Komponenten), die für die Installation des Updates erforderlich sind. Diese erforderlichen Komponenten können beispielsweise Updates des Betriebssystems sein.

  Wenn diese Option deaktiviert ist, müssen Sie die erforderlichen Komponenten möglicherweise manuell installieren.

  Diese Option ist standardmäßig deaktiviert.

- **Installation einer neuen Programmversion beim Update zulassen**

  Wenn diese Option aktiviert ist, 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 eine Aktualisierung 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 von Drittanbieter-Apps (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft entwickelt wurden) werden in den Ordner heruntergeladen, der im Feld **Ordner zum Herunterladen von Updates** angegeben ist.

  Wenn diese Option deaktiviert ist, werden die Updates automatisch auf dem Gerät installiert.

  Diese Option ist standardmäßig deaktiviert.

- **Ordner zum Herunterladen von Updates**

Dieser Ordner wird verwendet, um Updates von Drittanbieter-Apps (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft entwickelt wurden) herunterzuladen.

- **Erweiterte Diagnose aktivieren**

  Wenn diese Funktion aktiviert ist, führt der Administrationsagent die Ablaufverfolgung auch dann durch, wenn die Ablaufverfolgung für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center Cloud Console 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, beginnt der Administrationsagent sie wieder von vorn zu überschreiben. 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 Security Center Cloud Console durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

  Beim Erstellen einer Aufgabe, müssen Sie die erweiterte Diagnose nicht aktivieren. Sie möchten diese Funktion möglicherweise später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen empfangen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Dateien für die erweiterte Diagnose (MB)**

  Der Standardwert beträgt 100 MB und verfügbare Werte liegen zwischen 1 MB und 2048 MB. 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. Für das Abschließen des Vorgangs ist es erforderlich, ein Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten) neu zu starten. Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für die Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreies Arbeiten kritisch ist.

- **Gerät 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, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

- **Benutzer fragen**

Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und fordert den Benutzer auf, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterten Einstellungen definiert werden: Text der Nachricht für den Benutzer, die Anzeigehäufigkeit der Nachricht, sowie die Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, an denen Benutzer in der Lage sein müssen, den passendsten 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. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

  Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neu starten 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.

- **Wartezeit vor dem erzwungenen Schließen von Programmen in gesperrten Sitzungen (Min.)**

  Erzwungenes Schließen der Programmausführung, wenn das Gerät des Benutzers gesperrt ist (automatisch nach einer Phase der Inaktivität oder manuell).

  Wenn diese Option aktiviert ist, werden die Programme auf einem gesperrten Gerät nach Ablauf der im Eingabefeld angegebenen Zeitspanne automatisch geschlossen.

  Wenn diese Option deaktiviert ist, werden die 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 allgemeinen Aufgabeneinstellungen entsprechend Ihrer Bedürfnisse 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 Security Center Cloud Console 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 zur Installation von Updates oder des Assistenten zum 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)**. Damit werden alle Updates unabhängig von ihrem Genehmigungsstatus installiert. 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 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 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 Software-Updates, welche die Kriterien auf der Seite **Allgemeine Kriterien** des Assistenten erfüllen. Standardmäßig ausgewählt.

- Nur Updates aus der Liste installieren

  Es werden nur Software-Updates installiert, die Sie manuell aus der Liste auswählen. Diese Liste enthält alle verfügbaren Software-Updates.

  Sie können beispielsweise in den folgenden Fällen bestimmte Updates auswählen: um deren Installation in einer Testumgebung zu überprüfen, um nur kritische Apps zu aktualisieren oder um nur bestimmte Programme zu aktualisieren.

- Alle vorherigen Programm-Updates, die für die Installation der ausgewählten Updates erforderlich sind, automatisch installieren

Lassen Sie diese Option optimiert, wenn Sie mit der Installation von Programmzwischenversionen einverstanden sind, wenn 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 eine geradlinige Weist 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.

Wenn Sie beispielsweise Version 3 eines Programms auf einem Gerät installiert haben und Sie es auf Version 5 aktualisieren möchten, Version 5 dieses Programms aber nur über Version 4 installiert werden kann. 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)**. Damit werden alle Updates unabhängig von ihrem Genehmigungsstatus installiert. 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 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 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 **Apps** die Apps und Programmversionen aus, für die Sie Updates installieren möchten. Standardmäßig sind alle Programme ausgewählt.

5. Wählen Sie auf der Seite **Update-Kategorien** die Kategorien von Updates aus, die installiert werden sollen. Diese Kategorien sind dieselben wie 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)**. Damit werden alle Updates unabhängig von ihrem Genehmigungsstatus installiert. 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 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 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 **Apps** die Apps und Programmversionen aus, für die Sie Updates installieren möchten. Standardmäßig sind alle Programme ausgewählt.

5. Geben Sie im Fenster **Name** den Namen der Regel an, die Sie 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 Software-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 Security Center Cloud Console verwenden, und von dem Modus, in dem Kaspersky Security Center Cloud Console arbeitet.

Um die Aufgabe "Windows-Updates installieren" zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.
3. Wählen Sie für Kaspersky Security Center Cloud Console 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. Für das Abschließen des Vorgangs ist es erforderlich, ein Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten) neu zu starten. Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für die Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreies Arbeiten kritisch ist.

   - **Gerät 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, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

   - **Benutzer fragen**

     Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und fordert den Benutzer auf, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterten Einstellungen definiert werden: Text der Nachricht für den Benutzer, die Anzeigehäufigkeit der Nachricht, sowie die Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, an denen Benutzer in der Lage sein müssen, den passendsten 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. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neu starten 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 das Neustarten des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einer Textverarbeitungsanwendung bearbeitet wird und nicht gespeichert wurde, erlaubt die Anwendung keinen Neustart des Geräts.

  Wenn diese Option aktiviert ist, wird das Schließen solcher Anwendungen auf einem gesperrten Gerät erzwungen, bevor das Gerät neu gestartet wird. Das kann dazu führen, dass Benutzer ihre nicht gespeicherten 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, unter dem das Programm installiert und gestartet wurde, dass diese Aufgabe ausführt.

  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 dessen Namen 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 allgemeinen Aufgabeneinstellungen entsprechend Ihrer Bedürfnisse an.

14. Klicken Sie auf die Schaltfläche **Speichern**.

Die Aufgabe wird erstellt und konfiguriert.

Anzeigen von Informationen zu verfügbaren Software-Updates von Drittanbietern

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 Symbol **Filter** ( ) oben rechts in der Liste der Software-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 Software-Updates.

2. Daraufhin wird das Eigenschaftenfenster des Updates geöffnet, welches die in den folgenden Registerkarten gruppierte Informationen anzeigt:

   - **Allgemein**

Die Registerkarte zeigt allgemeine Informationen über das ausgewählte Update an:

- 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
- Installationsbedingungen, die vom Update vorgeschriebene werden
- Programmfamilie, zu der das Update gehört
- Programm, zu dem das Update gehört
- Revisionsnummer des Updates

- **Attribute**

  Diese Registerkarte zeigt eine Zusammenstellung von Eigenschaften des Updates an, die Sie verwenden können, um weitere Informationen über das Update zu erhalten. Die Zusammenstellung unterscheidet sich dabei je nachdem, ob es sich um ein Update von Microsoft oder von einem Drittthersteller handelt.

  Für ein Update von Microsoft zeigt die Registerkarte die folgenden Informationen an:

  - Ereignisstufe des Updates, entsprechend dem Microsoft Security Response Center (MSRC)
  - Link zu dem Artikel in der Microsoft Wissensdatenbank, in dem das Update beschrieben ist
  - Link zu dem Artikel in dem Microsoft Security Bulletin, in dem das Update beschrieben ist
  - Update-Identifikator (ID)

  Für ein Update eines Drittherstellers zeigt die Registerkarte die folgenden Informationen an:

  - Ob das Update ein Patch oder ein vollständiges Programmpaket darstellt
  - Lokalisierungssprache des Updates
  - On das Update automatisch oder manuell installiert wird
  - Ob das Update nach dessen Genehmigung widerrufen wurde
  - Link zum Download des Updates

- **Geräte**

  Diese Registerkarte zeigt eine Liste mit den Geräten an, auf denen das ausgewählte Update installiert wurde.

- Zu schließende Schwachstellen

  Diese Registerkarte zeigt eine Liste mit Schwachstellen an, die das ausgewählte Update schließen kann.

- Überschneidungen von Updates

  Diese Registerkarte zeigt Überschneidungen von verschiedenen, für das gleiche Programm veröffentlichten Updates an. Das heißt, ob das Update entweder 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 zeigt eine Liste mit den Aufgaben an, deren Aufgabenbereiche die Installation des ausgewählten Updates enthalten. Die Registerkarte ermöglicht es Ihnen außerdem, eine neue Aufgabe zur Remote-Installation für das Update zu erstellen.

Um die Statistik einer Updateinstallation anzuzeigen, gehen Sie wir folgt vor:

1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Softwareupdate.
2. Klicken Sie auf die Schaltfläche **Statistik über die Statuszustände der Update-Installation**.

   Das Diagramm mit dem Update-Installationsstatus wird angezeigt. Wenn Sie auf einen Status klicken, wird eine Liste der Geräte geöffnet, auf denen das Update den ausgewählten Status hat.

Sie können Informationen zu verfügbaren Software-Updates von Drittanbietern, einschließlich Microsoft, die auf dem ausgewählten verwalteten Windows-Gerät installiert ist, anzeigen.

Um eine Liste der verfügbaren Updates für Software von Drittanbietern, die auf dem ausgewählten verwalteten Gerät installiert ist, anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des Geräts, für das Sie Software-Updates von Drittanbietern 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 Software-Updates von Drittanbietern für das ausgewählte Gerät wird angezeigt.

Liste der verfügbaren Software-Updates in eine Datei exportieren

Sie können die angezeigte Liste der Updates für Drittanbieter-Software, einschließlich Microsoft-Software, 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 **Zeilen in TXT-Datei exportieren** oder **Zeilen in CSV-Datei exportieren**, je nachdem, welches Format für den Export bevorzugt wird.

Die Datei mit der Liste der verfügbaren Updates für Drittanbieter-Software, einschließlich Microsoft-Software, 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 Drittanbieter-Software-Updates.

2. Wählen Sie die Software-Updates aus, die Sie exportieren möchten.

   Überspringen Sie diesen Schritt, wenn Sie eine vollständige Liste der Software-Updates exportieren möchten.

   Wenn Sie eine vollständige Liste der Software-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 **Zeilen in TXT-Datei exportieren** oder **Zeilen in CSV-Datei exportieren**, je nachdem, welches Format für den Export bevorzugt wird.

Die Datei mit der Liste der Updates für Drittanbieter-Programme, einschließlich Microsoft-Software, die auf dem ausgewählten verwalteten Gerät installiert sind, wird auf das derzeit verwendete Gerät heruntergeladen.

Genehmigen und Ablehnen der Software-Updates von Drittanbietern

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 von den 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 mehrerer Updates können Sie die Regeln verwenden, die Sie in der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* konfigurieren können. Es wird empfohlen, den Status *Genehmigt* nur für die Updates zu setzen, die nicht den in den Regeln konfigurierten Kriterien entsprechen. Wenn Sie große Mengen an Updates manuell genehmigen, verringert sich die Leistungsfähigkeit des Administrationsservers, was zu einer Überlastung des Servers führen kann.

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.

Um ein Update in seinen Eigenschaften 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. 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 dem Ändern der Auto-Update-Einstellungen, wenden die Administrationsagenten die neuen Einstellungen auf jedes verwaltete Gerät an, auf dem 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. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry**.
2. Klicken Sie auf den Namen des Programms, für das Sie die Auto-Update-Einstellung ändern wollen.
   Um die Suche zu erleichtern, können Sie Liste mittels der Spalte **Status des automatischen Updates** filtern.
   Das Fenster mit den Programmeinstellungen wird geöffnet.
3. Legen Sie im Abschnitt **Allgemein** einen Wert für die folgende Einstellung fest:
   Status des automatischen Updates

   Wählen Sie eine der folgenden Varianten aus:

   - **Nicht definiert**

     Die Auto-Update-Funktion ist deaktiviert. Kaspersky Security Center Cloud Console 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 für das Programm ein Update veröffentlicht hat, wird dieses automatisch auf den verwalteten Geräten installiert. Es sind keine weiteren Aktionen erforderlich.

   - **Blockiert**

     Die Programm-Updates werden nicht automatisch installiert. Kaspersky Security Center Cloud Console 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-Einstellungen werden auf das ausgewählte Programm angewendet.

Schließen von Schwachstellen in Programmen von Drittanbietern

In diesem Abschnitt werden die Funktionen von Kaspersky Security Center Cloud Console beschrieben, die sich auf das Schließen von Schwachstellen in auf verwalteten Geräten installierten Programmen beziehen.

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 Programmen von Drittanbietern, einschließlich Microsoft-Programmen, 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 zum Schließen von Schwachstellen" starten, der automatisch eine dieser Aufgaben erstellt, oder Sie können eine dieser Aufgaben manuell erstellen.

   Anleitung: Beheben von Schwachstellen in Programmen von Drittanbietern, 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 geschlossenen 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 Software-Updates, welche die Kriterien der Regeln erfüllen, werden in die Datenverwaltungen der Verteilungspunkte heruntergeladen und werden installiert, um die Schwachstellen in Programmen zu beheben.

Wenn Sie die Aufgabe *Schwachstellen schließen* erstellt haben, werden nur Schwachstellen in Programmen von Microsoft behoben.

Über das Suchen und Schließen von Schwachstellen in Programmen

Kaspersky Security Center Cloud Console 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.

Finden von Schwachstellen in Programmen

Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console Software-Updates der Programmhersteller. Sie können jederzeit die Liste mit den Schwachstellen in Programmen anzeigen. Die Metadaten der Software-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 Security Center Cloud Console 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 Security Center Cloud Console werden Schwachstellen mithilfe *empfohlener Korrekturen* geschlossen. Empfohlene Korrekturen sind Software-Updates, deren Installation von Kaspersky-Spezialisten empfohlen wird.

Abhängig vom Modus der Kaspersky Security Center Cloud Console 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 Software-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 Prüfung von Dateien verwendet und umfassen die Untersuchung auf Viren, die statische und die dynamische Analyse, die Verhaltensanalyse in der Sandbox-Umgebung, sowie Machine Learning.

Kaspersky-Experten führen keine manuelle Analyse von Software-Updates von Drittanbietern durch, die mit der Funktion "Schwachstellen- und Patch-Management" installiert werden können. Darüber hinaus suchen Kaspersky-Experten weder nach Schwachstellen (bekannt und unbekannt) oder nicht dokumentierten Funktionen in derartigen Updates, noch führen sie an ihnen zusätzliche Analysen, neben denen, die im obigen Abschnitt genannt wurden, durch.

Die Aufgaben zur Installation von Software-Updates haben eine Reihe von Einschränkungen. Diese Einschränkungen sind abhängig von der Lizenz, unter der Sie Kaspersky Security Center Cloud Console verwenden, und von dem Modus, in dem Kaspersky Security Center Cloud Console 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.

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 Security Center Cloud Console verwenden, und von dem Modus, in dem Kaspersky Security Center Cloud Console 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 Schwachstellen in Programmen auf folgende Weise zu schließen:

- Öffnen Sie die Schwachstellenliste und geben Sie an, welche Schwachstellen geschlossen werden sollen.

  Infolgedessen wird eine neue Aufgabe zum Schließen von Schwachstellen in Programmen erstellt. Optional können Sie die ausgewählten Schwachstellen einer existierenden Aufgabe hinzufügen.

- Führen Sie den Assistenten zum Schließen von Schwachstellen aus.

  Die Verfügbarkeit dieser Funktion hängt vom Modus der Kaspersky Security Center Cloud Console 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 **Geräte** → **Verwaltete Geräte** → **<Gerätename>** → **Erweitert** → **Schwachstellen in Programmen**.
   - Um die Schwachstellenliste für ein bestimmtes Programm zu öffnen, wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry** → **<Programmname>** → **Schwachstellen**.

   Eine Seite mit der Liste von Schwachstellen in Programmen von Drittanbietern 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 Security Center Cloud Console 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 Security Center Cloud Console 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 **Geräte** → **Aufgaben** angezeigt. Wenn Sie sich entschieden haben, die Schwachstellen zu einer existierenden Aufgabe hinzuzufügen, werden die Schwachstellen in den Aufgabeneigenschaften gespeichert.

Um Schwachstellen in Programmen von Drittanbietern 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 Software-Updates manuell angeben, um die in den Aufgabeneinstellungen aufgelisteten Schwachstellen in Programmen zu schließen.

Schließen von Schwachstellen in Programmen mithilfe des Assistenten zum Schließen von Schwachstellen

Die Verfügbarkeit des Assistenten zum Schließen von Schwachstellen ist davon abhängig, welche Lizenz Sie verwenden und in welchem Modus Kaspersky Security Center Cloud Console ausgeführt wird.

Um Schwachstellen in Programmen mithilfe des Assistenten zum 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 zum 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 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 von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Schweregrad des ausgewählten Updates (**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 zum Schließen von Schwachstellen mithilfe von Updates des gleichen Typs wie das für die ausgewählte Schwachstelle empfohlene Update** (nur für Schwachstellen in Programmen von Microsoft verfügbar)
- **Regel zum Schließen von Schwachstellen in Programmen des ausgewählten Anbieters** (nur für Schwachstellen in Programmen von Drittanbietern verfügbar)
- **Regel zum Schließen von Schwachstellen in allen Versionen des ausgewählten Programms** (nur für Schwachstellen in Programmen von Drittanbietern 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 die Schaltfläche **Neue Aufgabe**.

  b. Konfigurieren Sie auf der sich öffnenden Seite die neue Regel:

  - Regel zum Schließen aller Schwachstellen der ausgewählten Signifikanz

    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 von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Schweregrad des ausgewählten Updates (**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 zum Schließen von Schwachstellen mithilfe von Updates des Typs** (nur für Schwachstellen in Programmen von Microsoft verfügbar)
- **Regel zum Schließen von Schwachstellen in Programmen des ausgewählten Anbieters** (nur für Schwachstellen in Programmen von Drittanbietern verfügbar)
- **Regel zum Schließen von Schwachstellen in allen Versionen des ausgewählten Programms** (nur für Schwachstellen in Programmen von Drittanbietern 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 existierenden 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 zum 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 Security Center Cloud Console 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 Security Center Cloud Console verwenden, und von dem Modus, in dem Kaspersky Security Center Cloud Console 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 **Geräte** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.
3. Wählen Sie für Kaspersky Security Center Cloud Console 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. Für das Abschließen des Vorgangs ist es erforderlich, ein Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten) neu zu starten. Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für die Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreies Arbeiten kritisch ist.

   - **Gerät 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, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

   - **Benutzer fragen**

     Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und fordert den Benutzer auf, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterten Einstellungen definiert werden: Text der Nachricht für den Benutzer, die Anzeigehäufigkeit der Nachricht, sowie die Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, an denen Benutzer in der Lage sein müssen, den passendsten 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. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

  Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neu starten 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 das Neustarten des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einer Textverarbeitungsanwendung bearbeitet wird und nicht gespeichert wurde, erlaubt die Anwendung keinen Neustart des Geräts.

  Wenn diese Option aktiviert ist, wird das Schließen solcher Anwendungen auf einem gesperrten Gerät erzwungen, bevor das Gerät neu gestartet wird. Das kann dazu führen, dass Benutzer ihre nicht gespeicherten 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, unter dem das Programm installiert und gestartet wurde, dass diese Aufgabe ausführt.

  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 dessen Namen 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 allgemeinen Aufgabeneinstellungen entsprechend Ihrer Bedürfnisse 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 Security Center Cloud Console 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 zur Installation von Updates oder den Assistenten zum 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 Software-Updates haben eine Reihe von Einschränkungen. Diese Einschränkungen sind abhängig von der Lizenz, unter der Sie Kaspersky Security Center Cloud Console verwenden, und von dem Modus, in dem Kaspersky Security Center Cloud Console arbeitet.

So erstellen Sie die Aufgabe Erforderliche Updates installieren und Schwachstellen schließen:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.

3. Wählen Sie für Kaspersky Security Center Cloud Console 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**

     Wenn diese Option aktiviert ist, werden Updates installiert, wenn das Gerät neu gestartet oder heruntergefahren wird. Anderenfalls werden Updates gemäß einem Zeitplan installiert.

     Verwenden Sie diese Option, wenn die Installation von Updates die Leistung des Geräts beeinträchtigen könnte.

     Diese Option ist standardmäßig deaktiviert.

   - **Erforderliche allgemeine Systemkomponenten installieren**

     Wenn diese Option aktiviert ist, installiert die Anwendung vor der Installation eines Updates automatisch alle allgemeinen Systemkomponenten (erforderlichen Komponenten), die für die Installation des Updates erforderlich sind. Diese erforderlichen Komponenten können beispielsweise Updates des Betriebssystems sein.

     Wenn diese Option deaktiviert ist, müssen Sie die erforderlichen Komponenten möglicherweise manuell installieren.

     Diese Option ist standardmäßig deaktiviert.

   - **Installation einer neuen Programmversion beim Update zulassen**

     Wenn diese Option aktiviert ist, 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 eine Aktualisierung 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 von Drittanbieter-Apps (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft entwickelt wurden) werden in den Ordner heruntergeladen, der im Feld **Ordner zum Herunterladen von Updates** angegeben ist.

Wenn diese Option deaktiviert ist, werden die Updates automatisch auf dem Gerät installiert.

Diese Option ist standardmäßig deaktiviert.

- **Ordner zum Herunterladen von Updates**

  Dieser Ordner wird verwendet, um Updates von Drittanbieter-Apps (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft entwickelt wurden) herunterzuladen.

- **Erweiterte Diagnose aktivieren**

  Wenn diese Funktion aktiviert ist, führt der Administrationsagent die Ablaufverfolgung auch dann durch, wenn die Ablaufverfolgung für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center Cloud Console 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, beginnt der Administrationsagent sie wieder von vorn zu überschreiben. 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 Security Center Cloud Console durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

  Beim Erstellen einer Aufgabe, müssen Sie die erweiterte Diagnose nicht aktivieren. Sie möchten diese Funktion möglicherweise später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen empfangen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Dateien für die erweiterte Diagnose (MB)**

  Der Standardwert beträgt 100 MB und verfügbare Werte liegen zwischen 1 MB und 2048 MB. 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. Für das Abschließen des Vorgangs ist es erforderlich, ein Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten) neu zu starten. Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für die Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreies Arbeiten kritisch ist.

- **Gerät 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, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und fordert den Benutzer auf, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterten Einstellungen definiert werden: Text der Nachricht für den Benutzer, die Anzeigehäufigkeit der Nachricht, sowie die Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, an denen Benutzer in der Lage sein müssen, den passendsten 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. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

  Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neu starten 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.

- **Wartezeit vor dem erzwungenen Schließen von Programmen in gesperrten Sitzungen (Min.)**

  Erzwungenes Schließen der Programmausführung, wenn das Gerät des Benutzers gesperrt ist (automatisch nach einer Phase der Inaktivität oder manuell).

  Wenn diese Option aktiviert ist, werden die Programme auf einem gesperrten Gerät nach Ablauf der im Eingabefeld angegebenen Zeitspanne automatisch geschlossen.

  Wenn diese Option deaktiviert ist, werden die 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 allgemeinen Aufgabeneinstellungen entsprechend Ihrer Bedürfnisse 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 Security Center Cloud Console 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 zur Installation von Updates oder des Assistenten zum 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)**. Damit werden alle Updates unabhängig von ihrem Genehmigungsstatus installiert. 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 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 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 Software-Updates, welche die Kriterien auf der Seite **Allgemeine Kriterien** des Assistenten erfüllen. Standardmäßig ausgewählt.

- **Nur Updates aus der Liste installieren**

  Es werden nur Software-Updates installiert, die Sie manuell aus der Liste auswählen. Diese Liste enthält alle verfügbaren Software-Updates.

  Sie können beispielsweise in den folgenden Fällen bestimmte Updates auswählen: um deren Installation in einer Testumgebung zu überprüfen, um nur kritische Apps zu aktualisieren oder um nur bestimmte Programme zu aktualisieren.

- **Alle vorherigen Programm-Updates, die für die Installation der ausgewählten Updates erforderlich sind, automatisch installieren**

Lassen Sie diese Option optimiert, wenn Sie mit der Installation von Programmzwischenversionen einverstanden sind, wenn 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 eine geradlinige Weist 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.

Wenn Sie beispielsweise Version 3 eines Programms auf einem Gerät installiert haben und Sie es auf Version 5 aktualisieren möchten, Version 5 dieses Programms aber nur über Version 4 installiert werden kann. 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)**. Damit werden alle Updates unabhängig von ihrem Genehmigungsstatus installiert. 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 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 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 **Apps** die Apps und Programmversionen aus, für die Sie Updates installieren möchten. Standardmäßig sind alle Programme ausgewählt.

5. Wählen Sie auf der Seite **Update-Kategorien** die Kategorien von Updates aus, die installiert werden sollen. Diese Kategorien sind dieselben wie 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)**. Damit werden alle Updates unabhängig von ihrem Genehmigungsstatus installiert. 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 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 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 **Apps** die Apps und Programmversionen aus, für die Sie Updates installieren möchten. Standardmäßig sind alle Programme ausgewählt.

5. Geben Sie im Fenster **Name** den Namen der Regel an, die Sie 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.

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** ( ) 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 Schwachstelle im Programm wird geöffnet.

Anzeigen von Informationen zu Schwachstellen in Programmen, die auf dem ausgewählten verwalteten Gerät erkannt wurden

Sie können Informationen zu Schwachstellen in Programmen, die auf dem ausgewählten verwalteten Windows-Gerät erkannt wurden, anzeigen.

Um eine Liste mit den Schwachstellen in Programmen auf dem ausgewählten verwalteten Gerät anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des Geräts, für das Sie erkannte Schwachstellen in Programmen 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**.

   Wenn Sie nur Schwachstellen in Programmen anzeigen möchten, die behoben werden können, wählen Sie die Option **Nur Schwachstellen anzeigen, die geschlossen werden können.**

Die Liste der Schwachstellen in Programmen, die auf dem ausgewählten verwalteten Gerät erkannt wurden, wird angezeigt.

Um Eigenschaften der ausgewählten Schwachstelle anzuzeigen, gehen Sie wie folgt vor:

Klicken Sie in der Liste der Schwachstellen in Programmen auf den Link mit dem Namen der Schwachstelle.

Das Eigenschaftenfenster der gewählten Schwachstelle wird geöffnet.

Anzeigen von Statistiken zu Schwachstellen auf verwalteten Geräten

Sie können Statistiken für jede Schwachstelle in Programmen auf verwalteten Geräten anzeigen. Die Statistik wird als Diagramm dargestellt. Das Diagramm zeigt die Anzahl der Geräte mit den folgenden Status an:

- *Ignoriert auf: <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn Sie in den Eigenschaften der Schwachstelle die Option zum Ignorieren der Schwachstelle manuell 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, sie jedoch noch nicht ausgeführt wurde.
- *Patch angewendet auf: <Anzahl der Geräte>*. Der Status wird zugewiesen, wenn Sie ein 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 verwalteten Geräten behoben wurde und auf den übrigen verwalteten Geräten ebenfalls behoben werden muss.

Um die Statistiken zur Schwachstelle auf einem verwalteten Gerät anzuzeigen, 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. 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 **Zeilen in TXT-Datei exportieren** oder **Zeilen 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 **Zeilen 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 Schwachstellen in Programmen ignorieren. Die Gründe für das Ignorieren von Schwachstellen in Programmen können beispielsweise folgende sein:

- Sie betrachten die Schwachstelle im Programm nicht als kritisch für Ihr Unternehmen.
- Sie vermuten, dass durch das Schließen von Schwachstellen in Programmen die Daten des Programms beschädigt werden können, welches das Schließen von Schwachstellen erforderlich macht.
- Sie sind sicher, dass die Schwachstelle im Programm keine Gefahr für das Netzwerk Ihres Unternehmens darstellt, da Sie andere Maßnahmen ergriffen haben, um Ihre verwalteten Geräte zu schützen.

Sie können eine Schwachstelle im Programm auf allen verwalteten Geräten oder nur auf den ausgewählten verwalteten Geräten ignorieren.

Um eine Schwachstelle im Programm auf allen verwalteten Geräten zu ignorieren, gehen Sie wie folgt vor:

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 Fenster mit den Eigenschaften der Schwachstelle im Programm öffnet sich.

3. Aktivieren Sie auf der Registerkarte **Allgemein** die Option **Schwachstelle ignorieren**.

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

   Das Fenster mit den Eigenschaften der Schwachstelle im Programm schließt sich.

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 **Geräte** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des Geräts, auf dem Sie eine Schwachstelle im Programm ignorieren möchten.

   Das Fenster mit den Geräteeigenschaften wird geöffnet.

3. Wählen Sie im Eigenschaftenfenster des Geräts die Registerkarte **Erweitert** aus.

4. Wählen Sie im linken Fensterbereich den Abschnitt **Schwachstellen in Programmen**.

   Die Liste der Schwachstellen in Programmen, die auf dem Gerät erkannt wurden, wird angezeigt.

5. Wählen Sie in der Liste der Schwachstellen in Programmen 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 Fenster mit den Geräteeigenschaften.

Die Schwachstelle im Programm wird auf dem ausgewählten Gerät ignoriert.

Die ignorierte Schwachstelle im Programm wird im Rahmen der Aufgabe *Schwachstellen schließen* oder *Erforderliche Updates installieren und Schwachstellen schließen* nicht behoben. Mit dem Filter können Sie ignorierte Schwachstellen in Programmen aus der Liste der Schwachstellen ausschließen.

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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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 Security Center Cloud Console für die Verwaltung von Programmen beschrieben, die auf Client-Geräten installiert sind.

Szenario: Programmverwaltung

Sie können den Start von Programmen auf Client-Geräten verwalten. Sie können zulassen oder blockieren, dass Programme auf verwalteten Geräten ausgeführt werden. Verwenden Sie dazu die Komponente "Programmkontrolle". Sie können nur Programme verwalten, die auf Windows- oder Linux-Geräten installiert sind.

Für Linux-basierte Betriebssysteme ist die Komponente "Programmkontrolle" beginnend mit Kaspersky Endpoint Security 11.2 für Linux verfügbar.

Erforderliche Vorrausetzungen

- Kaspersky Security Center Cloud Console 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 Programme auf Client-Geräten**

   Dieser Schritt unterstützt Sie dabei, herauszufinden, welche Programme auf den verwalteten Geräten installiert sind. Sie können die Liste der Programme anzeigen und gemäß den Sicherheitsrichtlinien Ihres Unternehmens entscheiden, welche Programme zulässig oder verboten sein sollen. Die Einschränkungen können sich auf die Informationssicherheitsrichtlinien des Unternehmens beziehen. Sie können diese Phase überspringen, wenn Sie genau wissen, welche Programme auf den verwalteten Geräten installiert sind.

   Anleitung: Liste der auf Client-Geräten installierten Anwendungen abrufen und anzeigen

2. **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. Sie können diesen Schritt überspringen, wenn Sie genau wissen, welche ausführbaren Dateien auf verwalteten Geräten installiert sind.

   Anleitung: Liste der auf Client-Geräten installierten ausführbaren Dateien abrufen und anzeigen

3. **Erstellen von Programmkategorien für die im Unternehmen verwendeten Programme**

Analysieren Sie die Listen der Programme und ausführbaren Dateien, die auf verwalteten Geräten gespeichert sind. Erstellen Sie Programmkategorien anhand der Analyse. Es wird empfohlen, die Kategorie "Arbeitsprogramme" zu erstellen, welche die Standardprogramme enthält, die im Unternehmen verwendet werden. Wenn verschiedene Benutzergruppen unterschiedliche Programmgruppen verwenden, können Sie für jede Benutzergruppe eine separate Programmkategorie erstellen.

Abhängig von den Kriterien zum Erstellen einer Programmkategorie können Sie zwei Typen von Programmkategorien erstellen.

Anleitung: Manuell zu erweiternde Programmkategorie erstellen, Programmkategorie mit ausführbaren Dateien aus ausgewählten Geräten erstellen

4. **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 Programmkategorien, die Sie in dem vorherigen Schritt erstellt haben.

   Anleitung: Konfigurieren der Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security für Windows

5. **Aktivieren der Komponente "Programmkontrolle" im Testbetrieb**

   Um sicherzustellen, dass die Regeln der Programmkontrolle nicht die für die Benutzerarbeit erforderlichen Programme 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 Anwendungen, 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.

6. **Ändern der Einstellungen für Programmkategorien 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

7. **Anwenden der Regeln der Programmkontrolle im Funktionsmodus**

   Nachdem die Regeln der "Programmkontrolle" getestet wurden und die Konfiguration der Programmkategorien komplett 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.

8. **Überprüfen der Konfiguration der Programmkontrolle**

   Stellen Sie folgende Punkte sicher:

   - Die Liste der Programmkategorien ist nicht leer. Prüfen Sie die Liste der Programmkategorien und stellen Sie sicher, dass sie die Kategorien enthält, die Sie angepasst haben.
   - Die "Programmkontrolle" wurde mithilfe der erstellten Programmkategorien angepasst. 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 von Programmen auf verwalteten Geräten gesteuert. Die Benutzer können nur Programme starten, die in Ihrem Unternehmen erlaubt sind. Im Unternehmen verbotene Programme 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

Informationen zur Programmkontrolle

Die Komponente "Programmkontrolle" überwacht die Versuche von Benutzern, Programme zu starten, und reguliert mithilfe der Regeln der "Programmkontrolle" den Start von Programmen.

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 Programmen, 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 Programme mit Ausnahme der in den Regeln zum Blockieren angegebenen Programme zulassen möchten. Der Modus *Deny-Liste* ist standardmäßig festgelegt.
- *Allow-Liste*. Dieser Modus wird verwendet, wenn Sie den Start aller Programme mit Ausnahme der in den Regeln zum Zulassen angegebenen Programme blockieren möchten.

Die Regeln der Programmkontrolle sind durch Programmkategorien implementiert. Sie erstellen Programmkategorien, die bestimmte Kriterien definieren. In Kaspersky Security Center Cloud Console gibt es zwei Arten von Programmkategorien:

- 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 Security Center Cloud Console 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 Programmliste aktualisiert hat.

Bei Windows-basierten Client-Geräten erhält der Administrationsagent die meisten Informationen über installierte Programme aus der Windows-Registrierung. Bei Linux-basierten Client-Geräten werden dem Administrationsagenten die Informationen über installierte Programme durch die Paketmanager bereitgestellt.

Um die Liste mit auf verwalteten Geräten installierten Programmen anzusehen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry**.

   Die Seite zeigt eine Tabelle mit den Programmen an, die auf verwalteten Geräten installiert sind. Wählen Sie ein Programm aus, um seine Eigenschaften anzeigen, z. B. Name des Anbieters, Versionsnummer, Liste der ausführbaren Dateien, Liste mit Geräten mit dem installierten Programm, Liste mit verfügbaren Software-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 Einstellungssymbol ( ) in der oberen rechten Ecke der Tabelle.

     Wählen Sie im geöffneten Menü **Spalten-Einstellungen** die Spalten aus, die in der Tabelle angezeigt werden sollen. Um den Betriebssystemtyp der Client-Geräte anzuzeigen, auf denen das Programm installiert ist, wählen Sie die Spalte **Typ des Betriebssystems** aus.

   - Klicken Sie auf das Filtersymbol ( ) 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 Programme wird angezeigt.

So zeigen Sie eine Liste der Programme an, die auf bestimmten verwalteten Geräten installiert sind:

Wechseln Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte** → **<Gerätename>** → **Erweitert** → **Programm-Registry**. In diesem Menü können Sie die Liste der Programme als csv- oder txt-Datei exportieren.

Ausführliche Informationen zur Programmkontrolle finden Sie in den folgenden Hilfethemen:

- Online-Hilfe von Kaspersky Endpoint Security für Windows
- Online-Hilfe von Kaspersky Endpoint Security für Linux

Abrufen und Anzeigen einer Liste der auf Client-Geräten installierten ausführbaren Dateien

Sie können eine Liste der auf verwalteten Geräten installierten ausführbaren Dateien abrufen. Um ausführbare Dateien zu inventarisieren, müssen Sie eine Inventarisierungsaufgabe erstellen.

Die Funktion zum Inventarisieren ausführbarer Dateien ist für die folgenden Programme verfügbar:

- Kaspersky Endpoint Security für Windows
- Kaspersky Endpoint Security für Linux (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.

Um eine Inventarisierungsaufgabe für ausführbare Dateien auf den Client-Geräten zu erstellen, gehen Sie folgendermaßen vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Aufgaben**.

   Die Aufgabenliste wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.

3. Wählen Sie auf der Seite **Neue Aufgabe** in der Dropdown-Liste **Programm** Kaspersky Endpoint Security für Windows oder Kaspersky Endpoint Security für Linux, in Abhängigkeit des Betriebssystemtyps der Client-Geräte.

4. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Inventarisierung**.

5. Klicken Sie auf der Seite **Erstellung der Aufgabe abschließen** auf **Fertigstellen**.

   Nach Abschluss des Assistenten für das Erstellen einer Aufgabe wird die Aufgabe **Inventarisierung** erstellt und 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.

Während der Inventarisierung werden die folgenden Formate von ausführbaren Dateien erkannt: mz, com, pe, ne, sys, cmd, bat, ps1, js, vbs, reg, msi, cpl, dll, jar, sowie html.

So zeigen Sie sich die Liste der auf Client-Geräten gespeicherten ausführbaren Dateien auf an:

Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Ausführbare Dateien**.

Auf der Seite wird die Liste der auf Client-Geräten installierten ausführbaren Dateien angezeigt.

Sie können die ausführbare Datei auch von einem verwalteten Gerät an Kaspersky senden, um nach potenziellen Bedrohungen zu suchen.

So senden Sie die ausführbare Datei vom verwalteten Gerät an Kaspersky:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Ausführbare Dateien**.
2. Klicken Sie auf den Link der ausführbaren Datei, die Sie an Kaspersky senden möchten.
3. Wechseln Sie im nächsten Fenster zum Abschnitt **Geräte** und aktivieren Sie anschließend das Kontrollkästchen des verwalteten Geräts, von dem Sie die ausführbare Datei senden möchten.

   Stellen Sie vor dem Senden der ausführbaren Datei durch das Aktivieren des Kontrollkästchens **Verbindung mit Administrationsserver nicht trennen** sicher, dass das verwaltete Gerät eine direkte Verbindung zum Administrationsserver besitzt. Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

4. Klicken Sie auf die Schaltfläche **An Kaspersky senden**.

Die ausgewählte ausführbare Datei wird heruntergeladen, um sie weiter an Kaspersky zu senden.

Erstellen einer manuell zu erweiternden Programmkategorie

Sie können einen Satz von Kriterien als Vorlage für ausführbare Dateien angeben, deren Start Sie in Ihrem Unternehmen zulassen oder blockieren möchten. Basierend auf ausführbaren Dateien, die den Kriterien entsprechen, können Sie eine Programmkategorie erstellen und diese in der Konfiguration der Programmkontrolle verwenden.

Um eine manuell zu erweiternde Programmkategorie zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programmkategorien**.

   Die Seite mit einer Liste der Programmkategorien wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Kategorie wird gestartet. Folgen Sie den Schritten des Assistenten.

3. Wählen Sie auf der Seite **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. Auf der Seite **Bedingungen** des Assistenten klicken Sie auf **Hinzufügen**, um ein Bedingungskriterium für das Aufnehmen von Dateien in die Kategorie aufzunehmen.
5. Wählen Sie auf der Seite **Bedingungskriterien** einen Regeltyp zum Erstellen einer Kategorie aus der Liste aus:

   - **Aus der KL-Kategorie**

     Wenn Sie diese Variante wählen, können Sie als Bedingung für die Aufnahme von Programmen in eine benutzerdefinierte Kategorie die Programmkategorie von Kaspersky angeben. Programme, die zur angegebenen Kaspersky-Kategorie gehören, werden in die benutzerdefinierte Programmkategorie aufgenommen.

   - **Zertifikat aus Datenverwaltung auswählen**

Wenn Sie diese Variante wählen, können Sie Zertifikate aus der Datenverwaltung für Zertifikate angeben. Ausführbare Dateien, die gemäß dem angegebenen Zertifikat signiert sind, werden zur Benutzerkategorie hinzugefügt.

- Pfad des Programms festlegen (Masken unterstützt)

  Wenn diese Option ausgewählt ist, können Sie den Pfad des Ordners auf dem Client-Gerät festlegen, der die ausführbaren Dateien enthält, die zur benutzerdefinierten Programmkategorie hinzugefügt werden sollen.

- Wechseldatenträger

  Wenn Sie diese Variante wählen, können Sie einen Datenträgertyp (beliebiger oder Wechseldatenträger) angeben, auf dem das Programm ausgeführt wird. Die auf dem ausgewählten Datenträgertyp ausgeführten Programme werden in die benutzerdefinierte Programmkategorie aufgenommen.

- **Hash, Metadaten oder Zertifikat**:

  - Aus Liste der ausführbaren Dateien auswählen

    Wenn Sie diese Variante wählen, können Sie die Programme, die in die Kategorie aufgenommen werden sollen, aus der Liste der ausführbaren Dateien des Client-Geräts auswählen.

  - Aus Programm-Registry auswählen

    Wenn diese Option ausgewählt ist, wird die Programm-Registry angezeigt. Sie können ein Programm aus der Registry auswählen und die folgenden Dateimetadaten angeben:

    - Dateiname.
    - Dateiversion. Sie können den genauen Wert der Version angeben oder eine Bedingung beschreiben, z. B. "größer als 5.0".
    - Programmname.
    - Programmversion. Sie können den genauen Wert der Version angeben oder eine Bedingung beschreiben, z. B. "größer als 5.0".
    - Hersteller.

  - Manuell angeben

Wenn Sie diese Option wählen, müssen Sie als Bedingung für die Aufnahme von Programmen in eine benutzerdefinierte Kategorie Datei-Hash, Metadaten oder Zertifikat angeben.

Dateihash

Je nach Version der Sicherheitsanwendung, die auf den Geräten in Ihrem Netzwerk installiert ist, müssen Sie einen Algorithmus auswählen, mit dem Kaspersky Security Center Cloud Console die Hash-Funktion für die Dateien der Kategorie berechnet. Die Informationen über die berechneten Hash-Funktionen werden in der Datenbank des Administrationsservers gespeichert. Das Speichern der Hash-Funktionen vergrößert geringfügig den Umfang der Datenbank.

SHA-256 ist eine kryptografische Hash-Funktion, in deren Algorithmen keine Schwachstellen gefunden wurden und sie daher momentan als die sicherste kryptographische Funktion betrachtet wird. Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher unterstützt die Berechnung der Hash-Funktion SHA-256. Die Berechnung der MD5-Hash-Funktion wird für die Programmversionen bis Kaspersky Endpoint Security 10 Service Pack 2 für Windows unterstützt.

Wählen Sie eine der Varianten zur Berechnung der Hash-Funktion für die Dateien der Kategorie durch Kaspersky Security Center Cloud Console aus:

- Wenn alle in Ihrem Netzwerk installierten Instanzen von Sicherheitsanwendungen das Programm Kaspersky Endpoint Security 10 Service Pack 2 für Windows oder höher darstellen, wählen Sie die das Kontrollkästchen **SHA-256** aus. Es ist nicht empfehlenswert, für Programmversionen vor Kaspersky Endpoint Security 10 Service Pack 2 für Windows eine Kategorie hinzuzufügen, die nach dem Kriterium "SHA-256-Hash" der 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 SHA-256 verwenden.

- Wenn verschiedene Geräte in Ihrem Netzwerk sowohl niedrigere als auch höhere Versionen von Kaspersky Endpoint Security 10 verwenden, wählen Sie die beiden Kontrollkästchen **SHA-256** und **MD5-Hash** aus.

Metadaten

Wenn diese Option ausgewählt ist, können Sie Dateimetadaten als Dateinamen, Dateiversion und Hersteller angeben. Die Metadaten werden an den Administrationsserver weitergegeben. Ausführbare Dateien mit denselben Metadaten werden in die Programmkategorie aufgenommen.

Zertifikat

Wenn Sie diese Variante wählen, können Sie Zertifikate aus der Datenverwaltung für Zertifikate angeben. Ausführbare Dateien, die gemäß dem angegebenen Zertifikat signiert sind, werden zur Benutzerkategorie hinzugefügt.

- Aus der Datei oder aus dem MSI-Paket / archiviertem Ordner

  Wenn Sie diese Variante wählen, können Sie als Bedingung für die Aufnahme von Programmen in eine benutzerdefinierte Kategorie eine MSI-Installationsdatei angeben. Die Metadaten des Installers werden an den Administrationsserver weitergegeben. Programme, deren Installer-Metadaten mit denen des MSI-Installers übereinstimmen, werden in die benutzerdefinierte Programmkategorie aufgenommen.

Das ausgewählte Kriterium wird zur Liste mit Kriterien hinzugefügt.

Sie können so viele Kriterien in die erstellende Programmkategorie aufnehmen, wie Sie benötigen.

6. Auf der Seite **Ausschlüsse** des Assistenten klicken Sie auf **Hinzufügen**, um ein exklusives Bedingungskriterium für das Ausschließen von Dateien in die Kategorie aufzunehmen, die gerade erstellt wird.

7. Wählen Sie auf der Seite **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 Programmkategorie erstellen und diese in der Konfiguration der Programmkontrolle verwenden.

Um eine Programmkategorie zu erstellen, die ausführbare Dateien von ausgewählten Geräten enthält, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programmkategorien**.

   Die Seite mit einer Liste der Programmkategorien wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Kategorie wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

3. Geben Sie auf der Seite **Methode zum Erstellen der Kategorie auswählen** des Assistenten 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** aus.

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 Programmkategorie verwendet werden sollen.

6. Geben Sie die folgenden Einstellungen an:

   - Algorithmus für die Berechnung der Hash-Funktion

Je nach Version der Sicherheitsanwendung, die auf den Geräten in Ihrem Netzwerk installiert ist, müssen Sie einen Algorithmus auswählen, mit dem Kaspersky Security Center Cloud Console die Hash-Funktion für die Dateien der Kategorie berechnet. Die Informationen über die berechneten Hash-Funktionen werden in der Datenbank des Administrationsservers gespeichert. Das Speichern der Hash-Funktionen vergrößert geringfügig den Umfang der Datenbank.

SHA-256 ist eine kryptografische Hash-Funktion, in deren Algorithmen keine Schwachstellen gefunden wurden und sie daher momentan als die sicherste kryptographische Funktion betrachtet wird. Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher unterstützt die Berechnung der Hash-Funktion SHA-256. Die Berechnung der MD5-Hash-Funktion wird für die Programmversionen bis Kaspersky Endpoint Security 10 Service Pack 2 für Windows unterstützt.

Wählen Sie eine der Varianten zur Berechnung der Hash-Funktion für die Dateien der Kategorie durch Kaspersky Security Center Cloud Console aus:

- Wenn alle in Ihrem Netzwerk installierten Instanzen von Sicherheitsanwendungen das Programm Kaspersky Endpoint Security 10 Service Pack 2 für Windows oder höher darstellen, wählen Sie die das Kontrollkästchen **SHA-256** aus. Es ist nicht empfehlenswert, für Programmversionen vor Kaspersky Endpoint Security 10 Service Pack 2 für Windows eine Kategorie hinzuzufügen, die nach dem Kriterium "SHA-256-Hash" der 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 SHA-256 verwenden.

Wenn verschiedene Geräte in Ihrem Netzwerk sowohl niedrigere als auch höhere Versionen von Kaspersky Endpoint Security 10 verwenden, wählen Sie die beiden Kontrollkästchen **SHA-256** und **MD5-Hash** aus.

Standardmäßig ist das Kontrollkästchen **SHA-256 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 Programmkategorie erstellt. Sie wird in der Liste der Programmkategorien angezeigt. Sie können die erstellte Programmkategorie verwenden, wenn Sie die "Programmkontrolle" anpassen.

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** → **Drittanbieter-Programme** → **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.

Konfigurieren der Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security für Windows

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 **Geräte** → **Richtlinien und Profile**.

   Eine Seite mit einer Liste der Richtlinien wird angezeigt.

2. Klicken Sie auf die Richtlinie **Kaspersky Endpoint Security für Windows**.

   Das Fenster mit den Richtlinieneinstellungen wird geöffnet.

3. Wechseln Sie zu **Programmeinstellungen → Sicherheitskontrollen → Programmkontrolle**.

   Das Fenster **Programmkontrolle** 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 Programmen 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 Programmstarts 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 des Programms ist im Testbetrieb untersagt** (*Infomeldungsereignis*). Dieses Ereignis wird angezeigt, wenn Sie die Programmkontrolle so konfiguriert haben, dass Regeln getestet werden.
- **Nachricht beim Verbot des Programmstarts an den Administrator** (*Warnungsereignis*). Dieses Ereignis wird angezeigt, wenn Sie in der "Programmkontrolle" das Anwenden von Regeln festgelegt haben, und ein Benutzer auf ein Programm zugreifen möchte, das beim Start blockiert wurde.

Es wird empfohlen, Ereignisauswahlen zu erstellen, um Ereignisse anzuzeigen, die sich auf den Betrieb der Programmkontrolle beziehen.

Sie können ausführbare Dateien, die sich auf Ereignisse der Programmkontrolle beziehen, zu einer vorhandenen Programmkategorie oder zu einer neuen Programmkategorie hinzufügen. Das Hinzufügen ausführbarer Dateien ist jedoch nur bei einer manuell zu erweiternden Programmkategorie möglich.

Um ausführbare Dateien, die sich auf Ereignisse der Programmkontrolle beziehen, zu einer Programmkategorie hinzuzufügen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung → Ereignisauswahlen**.

   Die Liste der Ereignisauswahlen wird angezeigt.

2. Wählen Sie die Ereignisauswahl aus, um Ereignisse im Zusammenhang mit der Programmkontrolle anzuzeigen und diese Ereignisauswahl zu starten.

   Wenn Sie keine Ereignisauswahl für die Programmkontrolle erstellt haben, können Sie eine vordefinierte Auswahl auswählen und starten, z. B. **Letzte Ereignisse**.

   Die Liste der Ereignisse wird angezeigt.

3. Wählen Sie die Ereignisse aus, für die Sie ausführbare Dateien der Programmkategorie hinzufügen möchten, und klicken Sie auf **Einer Kategorie zuweisen**.

   Der Assistent für das Erstellen einer Kategorie wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

4. Legen Sie auf der Seite des Assistenten die relevanten Einstellungen fest:

   - Wählen Sie im Abschnitt **Aktion mit der zum Ereignis gehörenden ausführbaren Datei** eine der folgenden Optionen aus:

     - **Zu neuer Programmkategorie hinzufügen**

       Wählen Sie diese Option, wenn Sie eine neue Programmkategorie basierend auf ereignisbezogenen ausführbaren Dateien erstellen möchten.

       Diese Variante ist standardmäßig ausgewählt.

       Wenn Sie diese Option ausgewählt haben, geben Sie einen neuen Kategorienamen an.

     - **Zu bestehender Programmkategorie hinzufügen**

       Wählen Sie diese Option, wenn Sie in einer bestehenden Programmkategorie ereignisbezogene ausführbare Dateien hinzufügen möchten.

       Diese Variante ist standardmäßig nicht ausgewählt.

       Wenn Sie diese Option ausgewählt haben, wählen Sie die Programmkategorie mit manuell hinzugefügtem Inhalt aus, zu der Sie ausführbare Dateien hinzufügen möchten.

   - Wählen Sie im Abschnitt **Regeltyp** eine der folgenden Optionen aus:

     - **Regeln zum Hinzufügen zu den Einschlüssen**
     - **Regeln zum Hinzufügen zu den Ausschlüssen**

   - Wählen Sie im Abschnitt **Als Bedingung verwendete Parameter** eine der folgenden Optionen aus:

     - **Zertifikatdetails (oder SHA-256-Hashs für Dateien ohne ein Zertifikat)**

       Die Dateien können vom Zertifikat signiert werden. Dabei können von einem Zertifikat mehrere Dateien signiert werden. Beispielsweise können verschiedene Versionen eines Programms von einem Zertifikat signiert sein oder mehrere verschiedene Programme 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.

       Jede Datei hat ihre eindeutige Hash-Funktion SHA-256. Bei der Auswahl der Hash-Funktion SHA-256 enthält die Kategorie nur die entsprechende Datei, beispielsweise die angegebene Programmversion.

       Wählen Sie diese Variante, wenn die Daten des Zertifikats einer ausführbaren Datei oder die Hash-Funktion SHA-256 für Dateien ohne Zertifikat zu den Regeln der Kategorie hinzugefügt werden müssen.

       Diese Variante ist standardmäßig ausgewählt.

     - **Zertifikatdetails (Dateien ohne ein Zertifikat werden übersprungen)**

Die Dateien können vom Zertifikat signiert werden. Dabei können von einem Zertifikat mehrere Dateien signiert werden. Beispielsweise können verschiedene Versionen eines Programms von einem Zertifikat signiert sein oder mehrere verschiedene Programme 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 die Zertifikatsdaten einer ausführbaren Datei zu den Regeln der Kategorie hinzugefügt werden müssen. Wenn die ausführbare Datei kein Zertifikat hat, wird eine solche Datei übersprungen. Die entsprechenden Informationen werden nicht zur Kategorie hinzugefügt.

- **Nur SHA-256 (Dateien ohne Hash werden übersprungen)**

  Jede Datei hat ihre eindeutige Hash-Funktion SHA-256. Bei der Auswahl der Hash-Funktion SHA-256 enthält die Kategorie nur die entsprechende Datei, beispielsweise die angegebene Programmversion.

  Wählen Sie diese Variante, wenn nur Daten der Hash-Funktion SHA-256 einer ausführbaren Datei zu den Regeln der Kategorie hinzugefügt werden müssen.

- **Nur MD5 (Modus eingestellt; Nur für die Version Kaspersky Endpoint Security 10 Service Pack 1)**

  Jede Datei hat ihre eindeutige MD5 Hash-Funktion. Bei der Auswahl der MD5 Hash-Funktion enthält die Kategorie nur die entsprechende Datei, beispielsweise die angegebene Programmversion.

  Wählen Sie diese Variante, wenn nur Daten der MD5 Hash-Funktion einer ausführbaren Datei zu den Regeln der Kategorie hinzugefügt werden müssen. 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

Programm-Tags

Dieser Abschnitt beschreibt die Programm-Tags und bietet eine Anleitung für deren Erstellung und Änderung sowie für das Zuweisen von Tags an Drittanbieter-Apps.

Über Programm-Tags

Kaspersky Security Center Cloud Console ermöglicht das Zuweisen von Tags zu Drittanbieter-Apps (Programme, die nicht von Kaspersky, sondern von anderen Softwareherstellern entwickelt wurden). Ein Tag ist eine Bezeichnung, anhand derer Programme gruppiert und gefunden werden können. Einem Programm zugewiesene Tags können als Bedingung in 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 Programm-Tag zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Tags**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Ein neues Tag-Fenster öffnet sich.
3. Geben Sie den Tag-Namen ein.
4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

Das neue Tag wird in der Liste der Programm-Tags angezeigt.

Programm-Tag umbenennen

Um ein Programm-Tag umzubenennen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Tags**.
2. Aktivieren Sie das Kontrollkästchen neben dem Tag, das Sie umbenennen möchten, und klicken Sie auf **Bearbeiten**.

   Ein Fenster mit den Tag-Eigenschaften wird geöffnet.
3. Ändern Sie den Tag-Namen.
4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

Das aktualisierte Tag wird in der Liste der Programm-Tags angezeigt.

Einem Programm Tags zuweisen

Um einem Programm ein oder mehrere Tags zuzuweisen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry**.
2. Klicken Sie auf den Namen des Programms, dem Sie Tags zuweisen möchten.

3. Wählen Sie die Registerkarte **Tags** aus.

   Die Registerkarte zeigt alle Programm-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. 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 dem Programm zugewiesen.

Zugewiesene Tags von einem Programm entfernen

Um ein oder mehrere Tags von einem Programm zu entfernen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry**.

2. Klicken Sie auf den Namen des Programms, von dem Sie Tags entfernen möchten.

3. Wählen Sie die Registerkarte **Tags** aus.

   Die Registerkarte zeigt alle Programm-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 vom Programm entfernt.

Die entfernten Tags werden nicht gelöscht. Bei Bedarf können Sie diese manuell löschen.

Programm-Tag löschen

Um ein Programm-Tag zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Tags**.

2. Wählen Sie in der Liste das Programm-Tag aus, das Sie löschen möchten.

3. Klicken Sie auf die Schaltfläche **Löschen**.

4. Klicken Sie im folgenden Fenster auf **OK**.

Das Programm-Tag wird gelöscht. Das gelöschte Tag wird automatisch von allen Programmen entfernt, denen es zugewiesen war.

Konfigurieren des Administrationsservers

Dieser Abschnitt beschreibt den Konfigurationsprozess und die Eigenschaften des Administrationsservers von Kaspersky Security Center Cloud Console.

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. Klicken Sie im Hauptmenü neben dem Namen des zukünftigen sekundären Administrationsservers auf das Einstellungen-Symbol ( ).

   b. Wechseln Sie auf der nächsten Seite mit Eigenschaften zum Abschnitt **Hierarchie der Administrationsserver** auf der Registerkarte **Allgemein**.

   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 **HDS-Serveradresse (des primären Administrationsservers in Cloud Console)** und **HDS-Serverports** die Adresse und den Port des primären Administrationsservers mit Kaspersky Security Center Cloud Console an.

      Die HDS-Serveradresse und HDS-Serverports finden Sie auf dem Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 neben dem Namen des zukünftigen primären Administrationsservers auf das Einstellungen-Symbol ( ).

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.

8. Füllen Sie auf der ersten Seite des Assistenten 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.

9. Wenn Sie einen Proxyserver für die Verbindung mit dem Kaspersky Security Center Cloud Console Administrationsserver (d.h. mit dem zukünftigen primären Server) verwenden, geben Sie dies und die Anmeldeinformationen des Proxyservers an.

10. Folgen Sie den weiteren Anweisungen 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.

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 **Geräte** → **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 **Geräte** → **Gruppenhierarchie**.
2. Klicken Sie auf die Schaltfläche **Importieren**.

   Daraufhin wird der Assistent für das Erstellen einer Administrationsgruppenstruktur gestartet. Folgen Sie den Anweisungen des Assistenten.

Speicherdauer von Ereignissen für die gelöschten Geräte konfigurieren

In Kaspersky Security Center Cloud Console 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 das Einstellungen-Symbol ( ) neben dem Namen des Kaspersky Security Center Cloud Console-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 Security Center Cloud Console und verwaltete Kaspersky-Programme 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 Security Center Cloud Console demselben Ereignistyp unterschiedliche Signifikanzen zuweisen.

Kaspersky Security Center Cloud Console versendet automatisch Benachrichtigungen über Ereignisse per E-Mail. Kaspersky Security Center Cloud Console 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 Security Center Cloud Console in bestimmten Zeiträumen Ereignisse mit derselben Signifikanz zusammen. Die Werte der Perioden werden von Kaspersky-Spezialisten verwaltet. Infolgedessen erhalten Empfänger zusammengefasste E-Mail-Nachrichten gemäß folgender Vorlage: "<Anzahl> <Signifikanz> (einschließlich niedrigerer Signifikanzen) Ereignisse sind aufgetreten".

Einschränkungen bei der Verwaltung von sekundären Administrationsservern, die lokal über Kaspersky Security Center Cloud Console ausgeführt werden

Nachdem Sie mithilfe der entsprechenden Option in Kaspersky Security Center Cloud Console 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 Security Center Cloud Console sind für den Benutzer nicht mehr verfügbar:

- In den Richtlinieneinstellungen von Administrationsagent und Administrationsserver sind die Registerkaten **Konfiguration von Ereignissen** und **Programmeinstellungen** nicht verfügbar. Es können keine neuen Richtlinien erstellt werden.
- In den Aufgabeneinstellungen von Administrationsagent und Administrationsserver sind die Registerkarten **Konfiguration von Ereignissen** und **Programmeinstellungen** 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 Programmversionen** 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:

Klicken Sie im Hauptmenü auf den Namen des Administrationsservers neben dem Einstellungen-Symbol ( ).

Eine Dropdown-Liste mit sekundären (einschl. virtuellen) Administrationsservern wird angezeigt.

Sie können auf den Namen eines dieser Administrationsserver klicken, um zu ihm zu wechseln.

Administrationsserver-Hierarchie löschen

Wenn Sie keine Hierarchie von Administrationsservern mehr verwenden möchten, können Sie diese von dieser Hierarchie trennen.

So löschen Sie eine Hierarchie von Administrationsservern:

1. Klicken Sie im Hauptmenü neben dem Namen des primären Administrationsservers auf das Einstellungen-Symbol ( ).
2. 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 Security Center Cloud Console 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 Security Center Cloud Console gemäß den derzeit verwendeten Funktionen:

1. Wechseln Sie im Hauptmenü zu Ihren Kontoeinstellungen und wählen Sie anschließend **Einstellungen der Benutzeroberfläche.**
2. Aktivieren oder deaktivieren Sie im folgenden Fenster **Einstellungen der Benutzeroberfläche** die Optionen:
   - **Verschlüsselung und Datenschutz anzeigen**

     Sie können diese Option zum Anzeigen oder Verbergen des Abschnitts **Vorgänge → Verschlüsselung und Datenschutz** in der Benutzeroberfläche verwenden. Kaspersky Security Center Cloud Console 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 und Berichterstattung → Vorfälle** in der Benutzeroberfläche verwenden. Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

2. Wechseln 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).
2. Wechseln Sie auf der nächsten Seite auf die Registerkarte **Administrationsserver**.
3. Wählen Sie den virtuellen Administrationsserver aus, den Sie aktivieren oder deaktivieren möchten.
4. Klicken Sie auf der Menüleiste auf die Schaltfläche **Virtuellen Administrationsserver aktivieren / deaktivieren**.

Der Status des virtuellen Administrationsservers ändert sich abhängig vom vorherigen Status zu "Aktiviert" oder "Deaktiviert". Der aktualisierte Status wird nehmen 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 Security Center Cloud Console anmelden.

Ein Administrator eines virtuellen Administrationsservers meldet sich an der Kaspersky Security Center Cloud Console genauso an, wie bei der Anmeldung am primären Administrationsserver. Kaspersky Security Center Cloud Console authentifiziert den Administrator und öffnet den virtuellen Administrationsserver, für den der Administrator die Zugriffsrechte besitzt. Der Administrator kann nicht zwischen Administrationsservern wechseln.

Erforderliche Vorrausetzungen

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

- Der virtuelle Administrationsserver wurde erstellt.
- Auf dem primären Administrationsserver haben Sie für den Administrator, den Sie dem virtuellen Administrationsserver zuweisen möchten ein Konto erstellt.
- 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 im Hauptmenü zum erforderlichen virtuellen Administrationsserver:
   a. Klicken Sie rechts neben dem Namen des aktuellen Administrationsservers auf das Chevron-Symbol ( ).
   b. Wählen Sie den gewünschten Administrationsserver aus.
2. Klicken Sie im Hauptmenü auf das Einstellungen-Symbol ( ) neben dem Namen des Administrationsservers.
   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
3. Klicken Sie auf der Registerkarte **Zugriffsrechte** auf die Schaltfläche **Hinzufügen**.
   Es öffnet sich eine zusammenfassende Liste der Benutzer des primären Administrationsservers und des aktuellen virtuellen Administrationsservers.
4. Wählen Sie aus der Benutzerliste das Konto des Administrators aus, das Sie dem virtuellen Administrationsserver zuweisen möchten, und klicken Sie anschließend auf die Schaltfläche **OK**.
   Die Anwendung fügt den ausgewählten Benutzer der Benutzerliste auf der Registerkarte **Zugriffsrechte** hinzu.
5. Aktivieren Sie das Kontrollkästchen neben dem hinzugefügten Konto und klicken Sie auf die Schaltfläche **Zugriffsrechte**.

6. Konfigurieren Sie die Rechte, die der Administrator auf dem virtuellen Administrationsserver bekommen soll.

   Um sich erfolgreich anzumelden, muss der Administrator mindestens über die folgenden Berechtigungen verfügen:

   - Berechtigung **Lesen** im Funktionsbereich **Allgemeine Funktionen → Basisfunktionen**
   - Berechtigung **Lesen** im Funktionsbereich **Allgemeine Funktionen → Virtuelle Administrationsserver**

Die Anwendung speichert die geänderten Benutzerrechte im Administratorkonto.

Konfigurieren der Zugriffsrechte durch Zuweisen von Benutzerrollen

Alternativ können Sie einem Administrator des virtuellen Administrationsservers die Zugriffsrechte über Benutzerrollen zuweisen. Dies kann beispielsweise nützlich sein, wenn Sie mehrere Administratoren auf demselben virtuellen Administrationsserver zuweisen möchten. In diesem Fall können Sie den Konten der Administratoren die gleiche oder mehrere Benutzerrollen zuweisen, anstatt für mehrere Administratoren die gleichen Benutzerrechte zu konfigurieren.

So weisen Sie einem virtuellen Administrationsserver einen Administrator durch Zuweisung von Benutzerrollen zu:

1. Erstellen Sie eine neue Benutzerrolle auf dem primären Administrationsserver und legen Sie anschließend alle erforderlichen Zugriffsrechte fest, die ein Administrator auf dem virtuellen Administrationsserver bekommen soll. Sie können mehrere Rollen anlegen, wenn Sie beispielsweise den Zugriff auf verschiedene Funktionsbereiche trennen möchten.
2. Wechseln Sie im Hauptmenü zum erforderlichen virtuellen Administrationsserver:
   a. Klicken Sie rechts neben dem Namen des aktuellen Administrationsservers auf das Chevron-Symbol (>).
   b. Wählen Sie den gewünschten Administrationsserver aus.
3. Weisen Sie die neue Rolle oder mehrere Rollen dem Administratorkonto zu.

Die Anwendung weist dem Administratorkonto die neue Rolle zu.

Konfigurieren der Zugriffsrechte auf Objektebene

Neben der Zuweisung von Zugriffsrechten auf Ebene von Funktionsbereichen können Sie auch den Zugriff auf bestimmte Objekte konfigurieren, die sich auf dem virtuellen Administrationsserver befinden, beispielsweise einer bestimmten Administrationsgruppe oder Aufgabe. Wechseln Sie dazu auf den virtuellen Administrationsserver und konfigurieren Sie anschließend die Zugriffsrechte in den Eigenschaften des Objekts.

Einen virtuellen Administrationsserver löschen

Wenn Sie einen virtuellen Administrationsserver löschen, werden alle Objekte, die auf dem virtuellen Administrationsserver erstellt wurden, inklusive Richtlinien und Aufgaben ebenfalls gelöscht. Die verwalteten Geräte aus den Administrationsgruppen, die von dem virtuellen Administrationsserver verwaltet wurden, werden von den Administrationsgruppen entfernt. Um die Geräte erneut in die Verwaltung durch Kaspersky Security Center Cloud Console aufzunehmen, müssen Sie eine Netzwerkabfrage durchführen und die gefundenen Geräte von der Gruppe "Nicht zugeordnete Geräte" in die Administrationsgruppe verschieben.

So löschen Sie einen virtuellen Administrationsserver:

1. Klicken Sie im Hauptmenü auf das Einstellungen-Symbol ( ) neben dem Namen des Administrationsservers.
2. Wechseln Sie auf der nächsten Seite auf die Registerkarte **Administrationsserver**.
3. Wählen Sie den virtuellen Administrationsserver aus, den Sie löschen möchten.
4. Klicken Sie auf der Menüleiste auf die Schaltfläche **Löschen**.

Der virtuelle Administrationsserver wurde gelöscht.

Überwachung und Berichterstattung

In diesem Abschnitt werden die Möglichkeiten für Monitoring und Berichte in Kaspersky Security Center Cloud Console beschrieben. Diese Möglichkeiten geben Ihnen einen Überblick über Ihre Infrastruktur, die Schutzstatus und Statistiken.

Nach der Bereitstellung von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console.

Erforderliche Vorrausetzungen

Nach der Verteilung von Kaspersky Security Center Cloud Console 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

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 Datenbank des Administrationsservers gespeichert. Basierend auf den Ereignissen bietet die Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console in dem Abschnitt **Überwachung und Berichterstattung** unter **Dashboard**.

Das Dashboard enthält Widgets, die angepasst werden können. Sie können aus einer großen Anzahl an unterschiedlichen Widgets auswählen, die als Kreis- oder Ringdiagramme, Tabellen, Grafiken, Balkendiagramme und Listen dargestellt werden. Die in den Widgets angezeigten Informationen werden automatisch aktualisiert und das Aktualisierungsintervall beträgt ein bis zwei Minuten. Das Aktualisierungsintervall unterscheidet sich von Widget zu Widget. Über das Einstellungsmenü können Sie die Daten eines Widgets jederzeit manuell aktualisieren.

Standardmäßig enthalten Widgets Informationen über alle Ereignisse, die in der Datenbank des Administrationsservers gespeichert sind.

Die Kaspersky Security Center Cloud Console besitzt eine Standardauswahl an Widgets der folgenden Kategorien:

- **Schutzstatus**
- **Softwareverteilung**
- **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.

Hinzufügen von Widgets zum Dashboard

So fügen Sie Widgets zum Dashboard hinzu:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.
2. Klicken Sie auf die Schaltfläche **Web-Widget hinzufügen oder wiederherstellen**.
3. Wählen Sie in der Liste der verfügbaren Widgets die Widgets aus, die Sie dem Dashboard hinzufügen möchten.

   Widgets sind nach Kategorien gruppiert. Um die Liste der in einer Kategorie enthaltenen Widgets anzuzeigen, klicken Sie auf den Richtungspfeil (>) 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.

Widget im Dashboard verbergen

So verbergen Sie ein angezeigtes Widget im Dashboard:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.
2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie ausblenden möchten.
3. Wählen Sie **Web-Widget verbergen** aus.
4. Klicken Sie im folgenden Fenster **Warnung** auf **OK**.

Das ausgewählte Widget wird verborgen. Später können Sie dieses Widget erneut zum Dashboard hinzufügen.

Verschieben eines Widgets auf dem Dashboard

So verschieben Sie ein Widget im Dashboard:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.
2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie verschieben möchten.

3. Wählen Sie **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.

Widget-Größe oder Darstellung ändern

Bei Widgets, die ein Diagramm anzeigen, können Sie dessen Darstellung ändern - ein Balkendiagramm oder Liniendiagramms. Bei einigen Widgets können Sie ihre Größe ändern: kompakt, mittel oder maximal.

So ändern Sie die Widget-Darstellung:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.

2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie bearbeiten möchten.

3. Führen Sie eine der folgenden Aktionen aus:

   - Um ein Widget als Balkendiagramm anzuzeigen, wählen Sie **Diagrammtyp: Balken** aus.
   - Um ein Widget als Liniendiagramm anzuzeigen, wählen Sie **Diagrammtyp: Linien** aus.
   - Um die vom Widget eingenommene Fläche zu ändern, wählen Sie einen der Werte:
     - **Kompakt**
     - **Kompakt (nur Balken)**
     - **Mittel (Donut-Diagramm)**
     - **Mittel (Balkendiagramm)**
     - **Maximum**

Die Darstellung des ausgewählten Widgets wird geändert.

Widget-Einstellungen ändern

Um die Einstellungen eines Widgets zu ändern, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.

2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie ändern möchten.

3. Wählen Sie **Einstellungen anzeigen** aus.

4. Ändern Sie im folgenden Fenster mit den Widgeteinstellungen die Widgeteinstellungen nach Bedarf.

5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die Einstellungen des ausgewählten Widgets werden geändert.

Der Satz an Einstellungen hängt vom jeweiligen Widget ab. Nachfolgend finden Sie einige allgemeine Einstellungen:

- **Gültigkeitsbereich des Web-Widgets** (Auswahl an Objekten, für die das Widget Informationen anzeigt) – Zum Beispiel eine Administrationsgruppe oder eine Geräteauswahl.
- **Aufgabe auswählen** (Aufgabe, für die das Widget Informationen anzeigt).
- **Zeitintervall** (Zeitintervall, während dem die Informationen im Widget angezeigt werden) – Zwischen zwei angegebenen Zeitpunkten; vom angegebenen Zeitpunkt bis zum aktuellen Tag; oder vom aktuellen Tag abzüglich der angegebenen Anzahl von Tagen bis zum aktuellen Tag.
- **Werte mit Status "Kritisch"** und **Werte mit Status "Warnung"** (Regeln, welche die Farbe einer Verkehrsampel festlegen).

Über den Nur-Dashboard-Modus

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

Wenn ein Benutzer im Nur-Dashboard-Modus arbeitet, gelten die folgenden Einschränkungen:

- Das Hauptmenü wird dem Benutzer nicht angezeigt, sodass er die Schutzeinstellungen für das Netzwerk nicht ändern kann.
- Der Benutzer kann mit Widgets keine Aktionen, wie hinzufügen oder ausblenden, ausführen. Daher müssen Sie alle für den Benutzer erforderlichen Widgets auf dem Dashboard platzieren und konfigurieren, indem Sie etwa die Regel zum Zählen von Objekten oder das Zeitintervall festlegen.

Sie können sich den Nur-Dashboard-Modus nicht selbst zuweisen. Wenn Sie in diesem Modus arbeiten möchten, wenden Sie sich an einen Systemadministrator, Managed Service Provider (MSP) oder einen Benutzer mit der Berechtigung **Objekt-ACLs ändern** im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen**.

Nur-Dashboard-Modus konfigurieren

Bevor Sie mit der Konfiguration des Nur-Dashboard-Modus beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Sie besitzen die Berechtigung **Objekt-ACLs ändern** in dem Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen**. Wenn Sie diese Berechtigung nicht besitzen, fehlt der Reiter zur Konfiguration des Modus.
- Der Benutzer besitzt die Berechtigungen **Lesen** in dem Funktionsbereich **Allgemeine Funktionen: Grundlegende Funktionen**.

Wenn in Ihrem Netzwerk eine Hierarchie von Administrationsservern eingerichtet ist, wechseln Sie zur Konfiguration des Nur-Dashboard-Modus auf den Server, auf dem das Benutzerkonto auf der Registerkarte **Benutzer** des Abschnitts **Benutzer und Rollen → Benutzer und Gruppen** verfügbar ist. Dabei kann es sich um einen primären oder einen physischen sekundären Server handeln. Es ist nicht möglich, den Modus auf einem virtuellen Server zu konfigurieren.

So konfigurieren Sie den Nur-Dashboard-Modus:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen → Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.

2. Klicken Sie auf den Namen des Benutzerkontos, für welches Sie das Dashboard mit Widgets anpassen möchten.

3. Öffnen Sie im folgenden Fenster mit den Kontoeinstellungen die Registerkarte **Dashboard**.

   Auf der sich öffnenden Registerkarte wird Ihnen das gleiche Dashboard angezeigt wie dem Benutzer.

4. Wenn die Option **Konsole im Nur-Dashboard-Modus anzeigen** aktiviert ist, klicken Sie auf den Umschalter, um sie zu deaktivieren.

   Wenn diese Option aktiviert ist, können auch Sie das Dashboard nicht ändern. Nachdem Sie die Option deaktiviert haben, können Sie Widgets verwalten.

5. Konfigurieren Sie das Erscheinungsbild des Dashboards. Der auf der Registerkarte **Dashboard** angezeigte Satz von Widgets steht dem Benutzer mit dem anpassbaren Konto zur Verfügung. Er oder sie kann weder die Einstellungen noch die Größe der Widgets ändern, und keine Widgets zum Dashboard hinzufügen oder daraus entfernen. Daher müssen Sie für den Benutzer die Widgets anpassen, damit er oder sie die Statistiken zum Netzwerkschutz anzeigen kann. Um dies zu tun, können Sie auf der Registerkarte **Dashboard** die gleichen Vorgänge mit den Widgets ausführen, wie im Abschnitt **Überwachung und Berichterstattung → Dashboard**:

   - Dem Dashboard neue Widgets hinzufügen.
   - Vom Nutzer nicht benötigte Widgets ausblenden.
   - Widgets verschieben, sodass sie einer bestimmten Reihenfolge entsprechen.
   - Die Größe oder das Aussehen von Widgets ändern.
   - Die Einstellungen von Widgets ändern.

6. Klicken Sie auf den Umschalter, um die Option **Konsole im Nur-Dashboard-Modus anzeigen** zu aktivieren.

   Anschließend steht dem Benutzer nur noch das Dashboard zur Verfügung. Er oder sie kann Statistiken überwachen, aber die Schutzeinstellungen des Netzwerks und das Erscheinungsbild des Dashboards nicht ändern. Da für Sie das gleiche Dashboard wie für den Benutzer angezeigt wird, können auch Sie das Dashboard nicht ändern.

   Wenn Sie die Option deaktiviert lassen, wird dem Benutzer das Hauptmenü angezeigt, sodass er verschiedene Aktionen in Kaspersky Security Center Cloud Console 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-Programmen spezielle Zugriffsrechte benötigt, konfigurieren Sie diese Rechte für den Benutzer. Anschließend werden für den Benutzer die Daten der Kaspersky-Programme in ihren entsprechenden Programm-Widgets angezeigt.

Der Benutzer kann sich jetzt mit dem angepassten Benutzerkonto an Kaspersky Security Center Cloud Console anmelden und die Statistiken zum Netzwerkschutz im Nur-Dashboard-Modus überwachen.

Berichte

In diesem Abschnitt wird beschrieben, wie Sie Berichte verwenden, benutzerdefinierte Berichtsvorlagen verwalten, Berichtsvorlagen zum Generieren neuer Berichte verwenden und Aufgaben zum Berichtsversand erstellen.

Berichte verwenden

Mithilfe von Berichten können Sie detaillierte, zahlenbasierte Informationen zur Sicherheit Ihres Unternehmensnetzwerkes zusammenstellen und diese Informationen in einer Datei speichern, per E-Mail versenden und ausdrucken.

Berichte finden Sie in der Kaspersky Security Center Cloud Console in dem Abschnitt **Überwachung und Berichterstattung** unter **Berichte**.

Standardmäßig enthalten Berichte Informationen für die letzten 30 Tage.

Die Kaspersky Security Center Cloud Console besitzt eine Standardauswahl an Berichten der folgenden Kategorien:

- **Schutzstatus**
- **Softwareverteilung**
- **Aktualisierungen**
- **Bedrohungsstatistiken**
- **Andere**

Sie können eigene Berichtsvorlagen erstellen, Berichtsvorlagen bearbeiten und löschen.

Sie können Berichte erstellen, die auf vorhandenen Vorlagen basieren, Berichte in eine Datei exportieren und Aufgaben zum Versand von Berichten erstellen.

Berichtsvorlage erstellen

Um eine Berichtsvorlage zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Berichte**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Daraufhin wird der Assistent für das Erstellen einer Berichtsvorlage gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.
3. Geben Sie auf der ersten Seite des Assistenten den Berichtsnamen ein und wählen Sie den Berichtstyp aus.

4. Wählen Sie auf der Seite **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 auf der Seite **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.

Anzeigen und Bearbeiten der Eigenschaften von Berichtsvorlagen

Sie können grundlegenden Eigenschaften einer Berichtsvorlage anzeigen und ändern, beispielsweise den Namen der Berichtsvorlage oder die im Bericht angezeigten Felder.

Um die Eigenschaften einer Berichtsvorlage anzuzeigen und zu ändern, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung → Berichte**.

2. Aktivieren Sie das Kontrollkästchen neben der Berichtsvorlage, deren Eigenschaften Sie anzeigen und ändern möchten.

   Alternativ dazu können Sie zuerst den Bericht generieren und dann auf die Schaltfläche **Bearbeiten** klicken.

3. Klicken Sie auf die Schaltfläche **Eigenschaften der Berichtsvorlage öffnen**.

   Das Fenster **Bearbeiten des Berichts <Berichtsname>** wird geöffnet, in dem die Registerkarte **Allgemein** ausgewählt ist.

4. Bearbeiten Sie die Berichtsvorlageneigenschaften:

   - Registerkarte **Allgemein**:
     - Name der Berichtsvorlage
     - Maximale Anzahl der angezeigten Einträge

Wenn diese Option aktiviert ist, übersteigt die Anzahl der Einträge in der Tabelle mit detaillierten Berichtsdaten den angegebene Wert nicht. 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 Security Center Cloud Console 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 der sekundären und virtuellen Administrationsserver einschließen**

  Wenn diese Option aktiviert ist, umfasst der Bericht die Informationen vom sekundären und vom virtuellen Administrationsserver, die dem Administrationsserver untergeordnet sind, für den die Berichtsvorlage erstellt wurde.

  Deaktivieren Sie diese Option, wenn Sie nur Daten vom aktuellen Administrationsserver anzeigen möchten.

  Diese Option ist standardmäßig aktiviert.

- **Bis Verschachtelungsebene**

Der Bericht enthält Daten von sekundären und virtuellen Administrationsservern, die sich unter dem aktuellen Administrationsserver auf der Verschachtelungsebene befinden, die kleiner oder gleich dem angegebenen Wert ist.

Als Standardwert ist 1 vorgegeben. Sie sollten diesen Wert ändern, wenn Sie Informationen von sekundären Administrationsservern sammeln müssen, die sich auf niedrigeren Ebenen in der Struktur befinden.

- **Intervall zum Warten auf Daten (Min.)**

  Vor Erstellen des Berichts wartet der Administrationsserver, für den die Berichtsvorlage erstellt wurde, während der angegebenen Anzahl von Minuten auf Daten von sekundären Administrationsservern. Wenn nach Ablauf dieses Zeitraums keine Daten von einem sekundären Administrationsserver eingehen, wird der Bericht dennoch ausgeführt. Anstelle der eigentlichen Daten zeigt der Bericht Daten aus dem Cache (wenn die Option **Daten von sekundären Administrationsservern im Cache zwischenspeichern** aktiviert ist) oder **N/A** (nicht verfügbar).

  Der Standardwert beträgt 5 (Minuten).

- **Daten von sekundären Administrationsservern im Cache zwischenspeichern**

  Sekundäre Administrationsserver übertragen regelmäßig Daten an den Administrationsserver, für den die Berichtsvorlage erstellt wird. Dort werden die übertragenen Daten im Cache gespeichert.

  Wenn der aktuelle Administrationsserver beim Erstellen des Berichts keine Daten von einem sekundären Administrationsserver empfangen kann, zeigt der Bericht Daten aus dem Cache an. Das Datum, an dem die Daten in den Cache übertragen wurden, wird ebenfalls angezeigt.

  Wenn Sie diese Option aktivieren, können Sie die Daten von sekundären Administrationsservern anzeigen, auch wenn die aktuellen Daten nicht mehr abgerufen werden können. Die angezeigten Daten können jedoch veraltet sein.

  Diese Option ist standardmäßig deaktiviert.

- **Häufigkeit des Cache-Updates (Std.)**

  Sekundäre Administrationsserver übertragen in regelmäßigen Abständen Daten an den Administrationsserver, für den die Berichtsvorlage erstellt wird. Sie können diesen Zeitraum in Stunden angeben. Wenn Sie 0 Stunden angeben, werden die Daten nur übertragen, wenn der Bericht generiert wird.

  Als Standardwert ist 0 vorgegeben.

- **Detaildaten 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 Security Center Cloud Console 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 und Berichterstattung → 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 und Berichterstattung → Berichte**.
2. Klicken Sie auf den Namen der Berichtsvorlage, die Sie zum Erstellen eines Berichts verwenden möchten.

Ein Bericht, der die ausgewählte Vorlage verwendet, wird erstellt angezeigt.

Berichtsdaten werden 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 und Berichterstattung → Berichte**.
2. [Optional] Aktivieren Sie die Kontrollkästchen neben den Berichtvorlagen, für die Sie eine Aufgabe zum Versand von Berichten erstellen möchten.
3. Klicken Sie auf die Schaltfläche **Neue Aufgabe für den Versand von Berichten**.
4. Der Assistent für das Erstellen einer Aufgabe wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

5. Geben Sie auf der ersten Seite des Assistenten den Aufgabennamen ein. Der Standardname ist **Berichtsversand (<N>)**, wobei <N> die laufende Nummer der Aufgabe ist.

6. Legen Sie auf der Seite mit Aufgabeneinstellungen des Assistenten die folgenden Einstellungen fest:

   a. Berichtsvorlagen, welche die Aufgabe versenden soll. Wenn Sie diese bereits in Schritt 2 ausgewählt haben, überspringen Sie diesen Schritt.

   b. Format der Berichte: HTML, XLS oder PDF.

   c. Ob die Berichte per E-Mail gesendet werden sollen; welche Einstellungen für die Benachrichtigung per E-Mail verwendet werden sollen.

7. Wenn Sie nach Erstellung der Aufgabe weitere Aufgabeneinstellungen bearbeiten möchten, aktivieren Sie auf der Seite **Erstellung der Aufgabe abschließen** des Assistenten die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen**.

8. Klicken Sie auf die Schaltfläche **Erstellen**, um die Aufgabe zu erstellen und den Assistenten zu beenden.

   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 Aufgabeneinstellungen geöffnet.

Berichtsvorlagen löschen

Um eine oder mehrere Berichtsvorlagen zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung → Berichte**.

2. Aktivieren Sie die Kontrollkästchen neben den Berichtsvorlagen, die Sie löschen möchten.

3. Klicken Sie auf die Schaltfläche **Löschen**.

4. Klicken Sie im folgenden Fenster auf **OK**, um die Auswahl zu bestätigen.

Die ausgewählten Berichtsvorlagen werden gelöscht. Wenn diese Berichtsvorlagen in Aufgaben zum Berichtsversand verwendet wurden, werden sie auch aus den entsprechenden Aufgaben entfernt.

Ereignisse und Ereignisauswahl

Dieser Abschnitt enthält Informationen zu Ereignissen und Ereignisauswahlen, zu den in den Komponenten von Kaspersky Security Center Cloud Console auftretenden Ereignistypen, und zur Verwaltung der Blockierung häufiger Ereignisse.

Über die Ereignisse in Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console ermöglicht das automatische Empfangen von Informationen über Ereignisse, die während der Ausführung des Administrationsservers und auf verwalteten Geräten installierter Programme von Kaspersky aufgetreten sind. Die Informationen über Ereignisse werden in der Datenbank des Administrationsservers gespeichert. 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 Security Center Cloud Console gibt es die folgenden Ereignistypen:

- Allgemeine Ereignisse. Diese Ereignisse kommen in allen verwalteten Kaspersky-Programmen 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-Programme. Jedes verwaltete Kaspersky-Programm 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 Security Center Cloud Console:
  - Administrationsserver
  - Administrationsagent
- Verwaltete Kaspersky-Programme

  Weitere Informationen zu den Ereignissen, die von verwalteten Kaspersky-Programmen generiert werden, finden Sie in der Dokumentation des entsprechenden Programms.

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 des Programms ohne Datenverlust oder eingeschränkter Funktionalität wiederhergestellt werden kann.

- *Infomeldung* – Ereignis, das zwecks Information über das erfolgreiche Ausführen einer Operation, die korrekte Ausführung des Programms oder den Abschluss einer Prozedur auftritt.

Für jedes Ereignis ist die Speicherdauer festgelegt, die in Kaspersky Security Center Cloud Console angezeigt oder geändert werden kann. Einige Ereignisse werden nicht standardmäßig in der Datenbank des Administrationsservers gespeichert, da die für sie definierte Speicherdauer gleich Null ist. In externe Systeme können nur jene Ereignisse exportieren, die mindestens einen Tag in der Datenbank des Administrationsservers gespeichert werden.

Ereignisse von Kaspersky Security Center Cloud Console

Jede Komponente von Kaspersky Security Center Cloud Console hat einen eigenen Satz von Ereignistypen. Dieser Abschnitt enthält eine Liste mit Ereignissen, die auf dem Administrationsserver von Kaspersky Security Center Cloud Console und im Administrationsagenten auftreten können. Die Typen der Ereignisse, die in den Programmen von Kaspersky auftreten, sind in diesem Abschnitt nicht aufgeführt.

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 konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

Datenstruktur der Ereignistypbeschreibung

Zu jedem Ereignistyp werden der dargestellte Name, der Identifikator (ID), der alphabetische Code, die Beschreibung und die Standard-Speicherdauer angezeigt.

- **Dargestellter Name des Ereignistyps**. Dieser Text wird in Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Datenbank des Administrationsservers 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 Security Center Cloud Console 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 konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

Ereignisse des Administrationsservers: Kritisch

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung
Lizenzbeschränkung wurde überschritten	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Einmal am Tag überprüft Kaspersky Security Center Cloud Console, o eine Lizenzbeschränkung überschritten wurde. Ereignisse dieser Art treten auf, wenn der Administrationsserver erkennt, dass Beschränkungen der Lizenz durch Kaspersky-Anwendungen, die auf den Client-Geräten installiert sind, überschritten werden. Außerdem tritt das Ereignis auf, wenn die Anzahl der aktuell genutzten Lizenzeinheite die von einer Lizenz abgedeckten werden, 110% der von der Lizenz abgedeckten Gesamtza an Einheiten überschreitet. Auch wenn dieses Ereigr eintritt, werden die Clien Geräte geschützt. Sie können auf dieses Ereignis folgendermaßer reagieren: • Schauen Sie sich die Liste der verwalteten Geräte an. Löschen

			Sie ungenutzte Geräte. • Stellen Sie eine Lizen für weitere Geräte zu Verfügung (fügen Sie dem Administrationsserve einen gültigen Aktivierungscode od eine Schlüsseldatei hinzu). Kaspersky Security Center Cloud Console ermittelt die Regeln zum Auslösen von Ereignisse wenn eine Lizenzbeschränkung überschritten wurde.
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 Schwellwe innerhalb eines kurzen Zeitraums überschreitet Sie können auf dieses Ereignis folgendermaßer reagieren: • Legen Sie den Schwellenwert in den Eigenschaften des Administrationsserve fest. • Erstellen Sie eine strengere Richtlinie, die aktiviert wird ode erstellen Sie eine Aufgabe, die bei Auftreten dieses Ereignisses ausgefüh wird.
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 Schwellwe innerhalb eines kurzen Zeitraums überschreitet Sie können auf dieses Ereignis folgendermaßer reagieren:

			• Legen Sie den Schwellenwert in den Eigenschaften des Administrationsserve fest. • Erstellen Sie eine strengere Richtlinie, die aktiviert wird ode erstellen Sie eine Aufgabe, die bei Auftreten dieses Ereignisses ausgeführ wird.
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 Schwellwe innerhalb eines kurzen Zeitraums überschreitet Sie können auf dieses Ereignis folgendermaßer reagieren: • Legen Sie den Schwellenwert in den Eigenschaften des Administrationsserve fest. • Erstellen Sie eine strengere Richtlinie, die aktiviert wird ode erstellen Sie eine Aufgabe, die bei Auftreten dieses Ereignisses ausgeführ wird.
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, warur der Administrationsagen auf diesem Gerät nicht ordnungsgemäß ausgeführt wird. Möglich Ursachen können Netzwerkprobleme oder das Entfernen des Administrationsagenten von diesem Gerät sein.
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.
Eingeschränkter Funktionsmodus	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Ereignisse dieser Art treten auf, wenn die Ausführung von Kaspersky Security Center Cloud Console n 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 Security Center Cloud Conso zu verwenden, stellen Sie eine Lizenz zur Verfügung (Fügen Sie dem Administrationsserve einen gültigen Aktivierungscode od eine Schlüsseldatei hinzu). • Der Administrationsserve verwaltet mehr Gerät als in der Lizenz angegeben. Verschieben Sie die

			Geräte aus der Administrationsgrupp des Administrationsserve in die eines anderen Administrationsserve (wenn das Lizenzlimit des anderen Administrationsserve dies zulässt).
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 Ta vor dem Ablaufdatum de Lizenz deaktiviert, so wir das Ereignis erst am darauf folgenden Tag veröffentlicht. Wenn die kommerzielle Lizenz abläuft, stellt Kaspersky Security Center Cloud Console n grundlegende Funktione bereit. Sie können auf dieses Ereignis folgendermaßer reagieren: • Vergewissern Sie sich dass dem Administrationsserve ein Reserve-Lizenzschlüssel hinzugefügt wurde. • Wenn Sie ein Abonnement verwenden, stellen Si sicher, dies zu Verlängern. Ein unbeschränktes

			Abonnement wird automatisch verlängert, falls der vereinbarte Betrag b zum Fälligkeitsdatum an den Dienstleister überwiesen wird.
Das Zertifikat ist abgelaufen	4132	KLSRV_CERTIFICATE_EXPIRED	Informationen werden demnächst hinzugefügt.
Updates der Programm-Module von Kaspersky wurden widerrufen	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Ereignisse dieser Art treten auf, wenn nahtlos Updates von den Kaspersky-Experten zurückgerufen wurden (für diese Updates wird der Status *Zurückgerufe* angezeigt); zum Beispiel, wenn Updates auf eine neuere Version aktualisiert werden müssen. Dieses Ereignis betrifft Patches von Kaspersky Security Center Cloud Console und keine Module von Anwendungen, die durch Kaspersky verwaltet werden. Das Ereignis gib den Grund an, warum da nahtlose Update nicht installiert wurde.

Ereignisse des Administrationsservers: Funktionsfehler

Die untenstehende Tabelle enthält die im Administrationsserver von Kaspersky Security Center Cloud Console 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 konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

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	4126	KLSRV_INVLICPROD_EXCEDED	Der Administrationsserver generiert Ereignisse dieser Art periodisch (stündlich). Ereignisse dieser Art treten auf, wenn Sie in Kaspersky	180 Tage

Installationen überschritten			Security Center Cloud Console 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-Programme von den Geräten, auf denen sie nicht verwendet werden. • Verwenden Sie eine Drittanbieter-Lizenz für mehr Geräte. Sie können die Lizenzschlüssel von Drittanbieter-Programmen verwalten, indem Sie die Funktionen der lizenzierten Programmgruppe verwenden. Zur lizenzierten Programmgruppe gehören Drittanbieter-Programme, welche die von Ihnen festgelegten Kriterien erfüllen.	

Ereignisse des Administrationsservers: Warnung

Die untenstehende Tabelle enthält die im Administrationsserver von Kaspersky Security Center Cloud Console 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 konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

Ereignisse des Administrationsservers: Warnung

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung
Lizenzbeschränkung wurde überschritten	4098	KLSRV_EV_LICENSE_CHECK_100_110	Einmal am Tag überprüf Kaspersky Security Center Cloud Console, eine Lizenzbeschränku überschritten wurde. Ereignisse dieser Art treten auf, wenn der Administrationsserver erkennt, dass Beschränkungen der Lizenz durch Kaspersky Anwendungen, die auf den Client-Geräten installiert sind, überschritten werden. Außerdem tritt das Ereignis auf, wenn die Anzahl der aktuell genutzten Lizenzeinhei die von einer Lizenz abgedeckten werden, 100% bis 110% der von Lizenz abgedeckten Gesamtzahl an Einheite überschreitet. Auch wenn dieses Ereig eintritt, werden die Clie Geräte geschützt. Sie können auf dieses Ereignis folgendermaße reagieren: • Schauen Sie sich die Liste der verwaltete Geräte an. Löschen Sie ungenutzte Geräte. • Stellen Sie eine Lize für weitere Geräte z Verfügung (fügen S dem Administrationserv einen gültigen Aktivierungscode o eine Schlüsseldatei hinzu).

			Kaspersky Security Center Cloud Cons ermittelt die Regeln zum Auslösen von Ereignissen wenn ei Lizenzbeschränkung überschritten wurde
Das Gerät war lange Zeit im Netzwerk inaktiv	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Informationen werden demnächst hinzugefüg
Konflikt von Gerätenamen	4102	KLSRV_EVENT_HOSTS_CONFLICT	Informationen werden demnächst hinzugefüg
Gerätestatus - "Warnung"	4114	KLSRV_HOST_STATUS_WARNING	Ereignisse dieser Art treten auf, wenn einem verwalteten Gerät der Status *Warnung* zugewiesen wird. Sie können die Bedingunge anpassen, unter denen der Gerätestatus zu *Warnung* wechselt.
Für eine der lizenzierten Programmgruppen wird die Beschränkung für die Anzahl von Installationen bald erreicht	4127	KLSRV_INVLICPROD_FILLED	Informationen werden demnächst hinzugefüg
Zertifikat wurde angefordert	4133	KLSRV_CERTIFICATE_REQUESTED	Informationen werden demnächst hinzugefüg
Zertifikat wurde entfernt	4134	KLSRV_CERTIFICATE_REMOVED	Informationen werden demnächst hinzugefüg
Das APNs-Zertifikat ist abgelaufen	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Informationen werden demnächst hinzugefüg
Das APNs-Zertifikat läuft bald ab	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Informationen werden demnächst hinzugefüg
Die FCM-Nachricht konnten nicht an das mobile Gerät gesendet werden	4138	KLSRV_GCM_DEVICE_ERROR	Informationen werden demnächst hinzugefüg
HTTP-Fehler beim Versenden der FCM-Nachricht an den FCM-Server	4139	KLSRV_GCM_HTTP_ERROR	Informationen werden demnächst hinzugefüg
Die FCM-Nachricht konnte nicht an den FCM-Server gesendet werden	4140	KLSRV_GCM_GENERAL_ERROR	Informationen werden demnächst hinzugefüg
Die Verbindung mit dem sekundären	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Informationen werden demnächst hinzugefüg

Administrationsserver wurde getrennt			
Die Verbindung mit dem primären Administrationsserver wurde getrennt	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Informationen werden demnächst hinzugefüg
KSN-Proxy wurde gestartet. Überprüfen der KSN-Verfügbarkeit nicht ausgeführt	7719	KSNPROXY_STARTED_CON_CHK_FAILED	Informationen werden demnächst hinzugefüg
Neue Updates der Programm-Module von Kaspersky sind registriert	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Informationen werden demnächst hinzugefüg
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 Ereigni aus der Datenbank des Administrationsservers begonnen hat, nachdem die Kapazitätsgrenze d Datenbank des Administrationsservers erreicht wurde. Sie können auf dieses Ereignis folgendermaße reagieren: • Ändern Sie die maximale Anzahl vo Ereignissen, die in d Datenbank des Administrationsserv gespeichert sind. • Verringern Sie die Li an Ereignissen, die i der Datenbank des Administrationsserv gespeichert werden sollen.
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 folgendermaße reagieren: • Ändern Sie die zulässige maximale Anzahl von Ereignissen, die in de Datenbank des Administrationsserv gespeichert sind. • Verringern Sie die Li an Ereignissen, die ir der Datenbank des Administrationsserv gespeichert werden sollen.
Die Lizenz läuft bald ab	4128	KLSRV_INVLICPROD_EXPIRED_SOON	Informationen werden demnächst hinzugefüg

Ereignisse des Administrationsservers: Information

Die untenstehende Tabelle enthält die im Administrationsserver von Kaspersky Security Center Cloud Console 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 konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

Ereignisse des Administrationsservers: Information

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer
Der Lizenzschlüssel ist zu über 90% verbraucht	4097	KLSRV_EV_LICENSE_CHECK_90	30 Tage
Neues Gerät wurde erkannt	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 Tage
Das Gerät wurde entsprechend einer Regel automatisch verschoben	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 Tage
Das Gerät wurde aus der Gruppe gelöscht: Lange Zeit im Netzwerk inaktiv	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 Tage
Die Beschränkung für die Anzahl von Installationen wird für eine der lizenzierten Programmgruppen bald	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 Tage

überschritten (mehr als 95% verbraucht)			
Es wurden Dateien gefunden, die zur Analyse an Kaspersky gesendet werden	4131	KLSRV_APS_FILE_APPEARED	30 Tage
Die ID der FCM Instance hat sich auf diesem mobilen Gerät geändert	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 Tage
Updates wurden erfolgreich in den angegebenen Ordner kopiert	4122	KLSRV_UPD_REPL_OK	30 Tage
Die Verbindung mit dem sekundären Administrationsserver wurde hergestellt	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 Tage
Die Verbindung mit dem primären Administrationsserver wurde hergestellt	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 Tage
Datenbanken wurden aktualisiert (In Kaspersky Security Center Cloud Console ist dieser Ereignistyp nur für einen sekundären Administrationsserver verfügbar.)	4144	KLSRV_UPD_BASES_UPDATED	30 Tage
KSN-Proxy wurde gestartet. Überprüfung 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: Objekt wurde modifiziert	4148	KLAUD_EV_OBJECTMODIFY	30 Tage
Audit: Objektstatus geändert	4150	KLAUD_EV_TASK_STATE_CHANGED	30 Tage
Audit: Gruppeneinstellungen modifiziert	4149	KLAUD_EV_ADMGROUP_CHANGED	30 Tage
Audit: Die Chiffrierschlüssel wurden vom Administrationsserver importiert oder exportiert	5100	KLAUD_EV_DPEKEYSEXPORT	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

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung
Fehler bei der Update-Installation	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Ereignisse dieser Art treten auf, wenn das Automatische Update un das Patchen von Komponenten von Kaspersky Security Cent Cloud Console nicht erfolgreich waren. Das Ereignis betrifft nicht die Updates von verwalteten Kaspersky-Programmen. Lesen Sie die Ereignisbeschreibung. Ein Windows-Problem auf dem Administrationsserv kann ein Grund für dieses Ereignis sein. Wenn die Beschreibung ein Problem in der Windows-Konfiguration erwähnt, beheben Sie dieses.
Installation des Updates für Drittherstellersoftware fehlgeschlagen	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Ereignisse dieser Art treten auf, wenn die Funktion "Schwachsteller und Patch-Management" sowie die Funktion "Verwaltung mobiler Geräte" verwendet werden, und wenn das Update einer Drittanbieter-Software nicht erfolgreich war.

			Überprüfen Sie, ob der Link zur Software für Drittanbieter gültig ist. Lesen Sie die Ereignisbeschreibung.
Installation der Updates von Windows-Update fehlgeschlagen	7717	KLNAG_EV_WUA_INSTALL_ERROR	Ereignisse dieser Art treten auf, wenn Window Updates nicht erfolgreich waren. Windows-Updates in der Richtlinie des Administrationsagenten anpassen. Lesen Sie die Ereignisbeschreibung. Suchen Sie nach dem Fehler in der Microsoft Knowledge Base. Wenden Sie sich an den technischen Support von Microsoft, wenn Sie das Problem nicht selbst lösen können.

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 konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

Ereignisse des Administrationsagenten: Warnung

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer
Während der Installation des Updates des Software-Moduls wurde eine Warnung zurückgegeben	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 Tage
Installation des Updates für die Drittherstellersoftware wurde mit einer Warnung abgeschlossen	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 Tage
Installation des Updates für Drittherstellersoftware wurde aufgeschoben	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 Tage
Es ist ein Vorfall aufgetreten	549	GNRL_EV_APP_INCIDENT_OCCURED	30 Tage
KSN-Proxy wurde gestartet. Überprüfen der	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 Tage

KSN-Verfügbarkeit nicht ausgeführt			

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 konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

Ereignisse des Administrationsagenten: Information

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standar Speicherd
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
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
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
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 Security Center Cloud Console verfügbar sind, erstellen und anzeigen.

Ereignisauswahlen finden Sie in Kaspersky Security Center Cloud Console in dem Abschnitt **Überwachung und Berichterstattung** unter **Ereignisauswahlen**.

Standardmäßig enthalten Ereignisauswahlen Informationen für die letzten sieben Tage.

Kaspersky Security Center Cloud Console besitzt eine Standardauswahl an vordefinierten Ereignisauswahlen:

- Ereignisse mit unterschiedlichen Ereigniskategorien:
  - **Kritische Ereignisse**
  - **Funktionsfehler**
  - **Warnungen**

- **Informative Ereignisse**

- **Benutzeranfragen** (Ereignisse der verwalteten Programme)
- **Letzte Ereignisse** (der letzten Woche)
- **Audit-Ereignisse**

  In Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Datenbank des Administrationsservers löschen

Ereignisauswahl erstellen

Um eine Ereignisauswahl zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Ereignisauswahlen**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Geben Sie im folgenden Fenster **Neue Ereignisauswahl** die Einstellungen der neuen Ereignisauswahl an. Tun Sie dies in einem oder mehreren der Abschnitte im Fenster.
4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

   Das Bestätigungsfenster öffnet sich.

5. Um das Ergebnis der Ereignisauswahl anzuzeigen, lassen Sie das Kontrollkästchen **Zum Auswahlergebnis wechseln** aktiviert.

6. Klicken Sie auf **Speichern**, um die Erstellung der Ereignisauswahl zu bestätigen.

Wenn Sie das Kontrollkästchen **Zum Auswahlergebnis wechseln** aktiviert lassen, wird das Ergebnis der Ereignisauswahl angezeigt. Andernfalls wird die neue Ereignisauswahl in der Liste der Ereignisauswahl angezeigt.

Ereignisauswahl bearbeiten

Um eine Ereignisauswahl zu bearbeiten, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Ereignisauswahlen**.

2. Aktivieren Sie das Kontrollkästchen neben der Ereignisauswahl, die Sie bearbeiten möchten.

3. Klicken Sie auf die Schaltfläche **Eigenschaften**.
   Ein Fenster mit den Einstellungen der Ereignisauswahl wird geöffnet.

4. Bearbeiten Sie die Eigenschaften der Ereignisauswahl.

   > Bei vordefinierten Ereignisauswahlen können Sie nur die Eigenschaften auf den folgenden Registerkarten bearbeiten: **Allgemein** (mit Ausnahme des Namens der Auswahl), **Uhrzeit** und **Zugriffsrechte**.

   Bei benutzerdefinierten Auswahlen können alle Eigenschaften bearbeitet werden.

5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die bearbeitete Ereignisauswahl wird in der Liste angezeigt.

Liste mit einer Ereignisauswahl anzeigen

Um eine Ereignisauswahl anzuzeigen:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Ereignisauswahlen**.

2. Aktivieren Sie das Kontrollkästchen neben der Ereignisauswahl, die Sie starten möchten.

3. Führen Sie eine der folgenden Aktionen aus:

   - Um die Sortierung der Ergebnisse der Ereignisauswahl anzupassen, gehen Sie wie folgt vor:

     a. Klicken Sie auf die Schaltfläche **Sortierung anpassen und starten**.

     b. Geben Sie im Fenster **Sortierung für Ereignisauswahl anpassen** die Einstellungen für die Sortierung an.

     c. Klicken Sie auf den Namen der Auswahl.

- Um die Liste der Ereignisse so anzuzeigen, wie sie auf dem Administrationsserver sortiert ist, klicken Sie auf den Namen der Auswahl.

Das Ergebnis der Ereignisauswahl wird angezeigt.

Ereignisauswahl exportieren

Mit Kaspersky Security Center Cloud Console können Sie eine Ereignisauswahl und deren Einstellungen in einer klo-Datei speichern. Sie können diese klo-Datei verwenden, um sowohl in Kaspersky Security Center Windows als auch in Kaspersky Security Center Linux die gespeicherte Ereignisauswahl zu importieren.

Beachten Sie, dass Sie nur benutzerdefinierte Ereignisauswahlen exportieren können. Ereignisauswahlen aus dem Standardumfang von Kaspersky Security Center Cloud Console (vordefinierte Auswahlen) können nicht in einer Datei gespeichert werden.

So exportieren Sie eine Ereignisauswahl:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Ereignisauswahlen**.
2. Aktivieren Sie das Kontrollkästchen neben der Ereignisauswahl, die Sie exportieren möchten.

   Sie können nicht mehrere Ereignisauswahlen gleichzeitig exportieren. Wenn Sie mehr als eine Auswahl auswählen, wird die Schaltfläche **Exportieren** deaktiviert.
3. Klicken Sie auf die Schaltfläche **Exportieren**.
4. Geben Sie im neuen Fenster **Speichern als** den Namen und den Pfad der Datei mit der Ereignisauswahl an und klicken Sie anschließend auf die Schaltfläche **Speichern**.

   Das Fenster **Speichern unter** wird nur angezeigt, wenn Sie Google Chrome, Microsoft Edge oder Opera verwenden. Wenn Sie einen anderen Browser verwenden, wird die Datei mit der Ereignisauswahl automatisch im Ordner **Downloads** gespeichert.

Ereignisauswahl importieren

Mit Kaspersky Security Center Cloud Console können Sie eine Ereignisauswahl aus einer klo-Datei importieren. Die klo-Datei enthält die exportierte Ereignisauswahl und deren Einstellungen.

So importieren Sie eine Ereignisauswahl:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Ereignisauswahlen**.
2. Klicken Sie auf die Schaltfläche **Importieren**, um eine Datei mit der Ereignisauswahl auszuwählen, die Sie importieren möchten.
3. Geben Sie im folgenden Fenster den Pfad zur klo-Datei an und klicken Sie anschließend auf die Schaltfläche **Öffnen**. Beachten Sie, dass Sie nur eine Ereignisauswahl-Datei auswählen können.

   Die Verarbeitung der Ereignisauswahl beginnt.

Die Benachrichtigung mit dem Resultat des Imports wird angezeigt. Wenn die Ereignisauswahl erfolgreich importiert wurde, können Sie auf den Link **Importdetails anzeigen** klicken, um die Eigenschaften der Ereignisauswahl anzuzeigen.

Nach einem erfolgreichem 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

Um Informationen zu einem Ereignis anzuzeigen, gehen Sie wie folgt vor:

1. Starten einer 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

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.
3. Klicken Sie auf die Schaltfläche **In Datei exportieren**.

Das ausgewählte Ereignis wird in eine 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 Security Center Cloud Console gespeichert sind. Standardmäßig verfügen 1.000 Geräte über 100.000 Ereignisse. Wird diese Grenze überschritten, werden alten 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 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 Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console einnehmen.

Ereignisse löschen

Um eine oder mehrere Ereignisse zu löschen, gehen Sie wie folgt vor:

1. Starten einer Ereignisauswahl.
2. Aktivieren Sie die Kontrollkästchen neben den gewünschten Ereignissen.
3. Klicken Sie auf die Schaltfläche **Löschen**.

Die ausgewählten Ereignisse werden gelöscht und können nicht wiederhergestellt werden.

Ereignisauswahl löschen

Sie können nur benutzerdefinierte Ereignisauswahlen löschen. Vordefinierte Ereignisauswahlen können nicht gelöscht werden.

Um eine oder mehrere Ereignisauswahlen zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Ereignisauswahlen**.
2. Aktivieren Sie die Kontrollkästchen neben den Ereignisauswahlen, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie im folgenden Fenster auf **OK**.

Die Ereignisauswahl ist gelöscht.

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

Kaspersky Security Center Cloud Console 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.

Einstellungen zum Umschalten der Status von Geräten

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 **Geräte** → **Gruppenhierarchie**.
2. Klicken Sie in der angezeigten Liste der Gruppen auf den Link mit dem Namen der Gruppe, für die Sie den Wechsel der Gerätestatus ändern möchten.
3. Klicken Sie im daraufhin geöffneten Eigenschaftenfenster auf die Registerkarte **Gerätestatus**.
4. Wählen Sie im linken Fensterbereich die Option **Kritisch** aus.
5. Aktivieren Sie im rechten Bereich im Abschnitt **Werte, für die der Status auf "Kritisch" gesetzt wird** die Bedingung zum Umschalten eines Geräts in den Status *Kritisch*.

   Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

6. Aktivieren Sie das Optionsfeld neben der Bedingung in der Liste.
7. Klicken Sie in der oberen linken Ecke der Liste auf die Schaltfläche **Bearbeiten**.
8. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.

   Es können nicht für alle Bedingungen Werte festgelegt werden.

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

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Kritisch*.

Um die Änderungen des Gerätestatus auf Warnung zu aktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Gruppenhierarchie**.
2. Klicken Sie in der angezeigten Liste der Gruppen auf den Link mit dem Namen der Gruppe, für die Sie den Wechsel der Gerätestatus ändern möchten.
3. Klicken Sie im daraufhin geöffneten Eigenschaftenfenster auf die Registerkarte **Gerätestatus**.
4. Wählen Sie im linken Fensterbereich die Option **Warnung** aus.
5. Aktivieren Sie im rechten Bereich im Abschnitt **Werte, für die der Status auf "Warnung" gesetzt wird** die Bedingung zum Umschalten eines Geräts in den Status *Warnung*.

Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

6. Aktivieren Sie das Optionsfeld neben der Bedingung in der Liste.
7. Klicken Sie in der oberen linken Ecke der Liste auf die Schaltfläche **Bearbeiten**.
8. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.

   Es können nicht für alle Bedingungen Werte festgelegt werden.
9. Klicken Sie auf die Schaltfläche **OK**.

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Warnung*.

Einstellungen für das Versenden von Benachrichtigungen anpassen

In Kaspersky Security Center Cloud Console können Sie E-Mail-Benachrichtigung über auftretende Ereignisse konfigurieren.

So können Sie in Kaspersky Security Center Cloud Console Benachrichtigung über auftretende Ereignisse konfigurieren:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.
2. 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 Security Center Cloud Console 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 Security Center Cloud Console auftreten.

Für die Einstellungen des Administrationsservers, einer Richtlinie oder des Programms können Sie im Abschnitt **Konfiguration von Ereignissen** die Benachrichtigungseinstellungen für bestimmte Ereignisse überschreiben.

Kaspersky-Mitteilungen

In diesem Abschnitt wird beschrieben, wie Sie Kaspersky-Mitteilungen verwenden, konfigurieren und deaktivieren.

Über Kaspersky-Mitteilungen

Im Abschnitt mit den Kaspersky-Mitteilungen (**Überwachung und Berichterstattung → Mitteilungen von Kaspersky**) finden Sie Wissenswertes zu Kaspersky Security Center Cloud Console und den verwalteten Programmen, die auf den verwalteten Geräten installiert sind. Kaspersky Security Center Cloud Console aktualisiert die Informationen in diesem Abschnitt regelmäßig: Veraltete Mitteilungen werden entfernt und neue Informationen hinzugefügt.

Kaspersky Security Center Cloud Console zeigt nur die Kaspersky-Mitteilungen an, die sich auf den derzeit verbundenen Administrationsserver und die auf dessen verwalteten Geräten installierten Kaspersky-Programme beziehen. Die Mitteilungen werden für jeden Typ von Administrationsserver individuell angezeigt – primär, sekundär oder virtuell.

Wenn Kaspersky Security Center Cloud Console von mehreren Administratoren verwendet wird und diese unterschiedliche Sprachen für die Benutzeroberfläche einstellen, zeigt Kaspersky Security Center Cloud Console 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 Konsole abgemeldet und erneut angemeldet haben.

Die Mitteilungen enthalten Informationen der folgenden Typen:

- Sicherheitsrelevante Mitteilungen

  Mit sicherheitsrelevanten Mitteilungen werden die in Ihrem Netzwerk installierten Kaspersky-Programme auf dem neuesten Stand und voll funktionsfähig gehalten. Die Mitteilungen können Informationen über kritische Updates für Kaspersky-Programme, Korrekturen für gefundene Schwachstellen und Methoden zum Beheben sonstiger Probleme in Kaspersky-Programmen enthalten. Sicherheitsrelevante Mitteilungen sind standardmäßig aktiviert. Wenn Sie keine Mitteilungen erhalten möchten, können Sie diese Funktion deaktivieren.

  > Im Testmodus von Kaspersky Security Center Cloud Console können Sie die sicherheitsrelevanten Mitteilungen nicht deaktivieren.

  Um Ihnen die Informationen anzuzeigen, die der Konfiguration Ihres Netzwerkschutzes entsprechen, sendet Kaspersky Security Center Cloud Console Daten an die Kaspersky-Cloud-Server und empfängt nur die Mitteilungen, welche die in Ihrem Netzwerk installierten Kaspersky-Programme betreffen. Der Umfang an Daten, der an die Server gesendet werden kann, ist in der Vereinbarung zur Kaspersky Security Center Cloud Console beschrieben, die Sie beim Erstellen eines Unternehmensarbeitsbereichs akzeptieren.

- Marketing-Mitteilungen

  Marketing-Mitteilungen enthalten Informationen über Sonderangebote für Ihre Kaspersky-Programme, Werbung und Neuigkeiten von Kaspersky. Marketing-Mitteilungen sind standardmäßig deaktiviert. Diese Art von Mitteilungen erhalten Sie nur, wenn Sie Kaspersky Security Network (KSN) aktiviert haben. Sie können Marketing-Mitteilungen deaktivieren, indem Sie KSN deaktivieren.

  Um Ihnen nur relevante Informationen anzuzeigen, die für den Schutz Ihrer Netzwerkgeräte und für Ihren Aufgabenbereich hilfreich sein können, sendet Kaspersky Security Center Cloud Console Daten an die Kaspersky-Cloud-Server und empfängt die entsprechenden Mitteilungen. Der Datensatz, der an die Server gesendet werden kann, wird im Abschnitt "Verarbeitete Daten" der KSN-Erklärung beschrieben.

Neue Informationen werden in Abhängigkeit ihrer Wichtigkeit in zwei Kategorien eingeteilt:

1. Kritische Information
2. Wichtige Neuigkeiten
3. Warnung
4. Information

Wenn im Abschnitt "Mitteilungen von Kaspersky" neue Informationen erscheinen, zeigt Kaspersky Security Center Cloud Console ein Benachrichtigungssymbol an, welches der Ereigniskategorie der Mitteilungen entspricht. Sie können auf das Symbol klicken, um sich die Mitteilung im Abschnitt "Mitteilungen von Kaspersky" anzusehen.

Kaspersky-Mitteilungen deaktivieren

Im Abschnitt Mitteilungen von Kaspersky (**Überwachung und Berichterstattung → Mitteilungen von Kaspersky**) finden Sie Wissenswertes zu Ihrer Version von Kaspersky Security Center Cloud Console und den verwalteten Programmen, die auf Ihren verwalteten Geräten installiert sind. Wenn Sie keine Mitteilungen von Kaspersky erhalten möchten, können Sie diese Funktion deaktivieren.

Die Kaspersky-Mitteilungen enthalten zwei Arten von Informationen: sicherheitsrelevante Mitteilungen und Marketing-Mitteilungen. Sie können jeden Mitteilungstyp getrennt deaktivieren.

> Im Testmodus von Kaspersky Security Center Cloud Console können Sie die sicherheitsrelevanten Mitteilungen nicht deaktivieren.

Um sicherheitsrelevante Mitteilungen zu deaktivieren:

1. Klicken Sie im Hauptmenü auf das Einstellungen-Symbol ( ) neben dem Namen des Administrationsservers.
   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Mitteilungen von Kaspersky** aus.
3. Stellen Sie den Umschalter auf die Position **Sicherheitsrelevante Mitteilungen Deaktiviert**.
4. Klicken Sie auf die Schaltfläche **Speichern**.
   Jetzt sind die Kaspersky-Mitteilungen deaktiviert.

Marketing-Mitteilungen sind standardmäßig deaktiviert. Marketing-Mitteilungen erhalten Sie nur, wenn Sie Kaspersky Security Network (KSN) aktiviert haben. Sie können diese Art von Mitteilungen deaktivieren, indem Sie KSN deaktivieren.

Um Marketing-Mitteilungen zu deaktivieren:

1. Klicken Sie im Hauptmenü auf das Einstellungen-Symbol ( ) neben dem Namen des Administrationsservers.
   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN-Einstellungen** aus.
3. Deaktivieren Sie die Option **Ich akzeptiere die Nutzungsbedingungen für Kaspersky Security Network**.

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

   Jetzt sind die Marketing-Mitteilungen deaktiviert.

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 das Einstellungen-Symbol ( ) neben dem 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.

Ereignisse in SIEM-Systeme exportieren

Dieser Abschnitt beschreibt, wie Sie den Export von Ereignissen in ein SIEM-System konfigurieren.

Szenario: Den 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 externe SIEM-Systeme ermöglicht den Administratoren der SIEM-Systeme, sofort auf die Ereignisse des Sicherheitssystems, die auf den verwalteten Geräten oder auf Geräten aus Gruppen auftreten, zu reagieren.

Erforderliche Vorrausetzungen

Bevor Sie mit der Konfiguration des Ereignisexports in die Kaspersky Security Center Cloud Console 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 Security Center Cloud Console empfängt**

  Sie müssen im SIEM-System das Empfangen von Ereignissen von Kaspersky Security Center Cloud Console 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-Programmen auftreten. Darüber hinaus können Sie Ereignisse für bestimmte verwaltete Kaspersky-Anwendungen markieren.

- **Konfiguration von Kaspersky Security Center Cloud Console für den Export an ein SIEM-System**

  Sie müssen Kaspersky Security Center Cloud Console 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 Security Center Cloud Console müssen einige Einstellungen des SIEM-Systems angegeben werden. Es ist empfehlenswert, diese Einstellungen im Voraus zu bestimmen, damit die Einstellungen für Kaspersky Security Center Cloud Console vorbereitet werden können.

Für die Einstellungen des automatischen Ereignisexports ins SIEM-System müssen die Werte der folgenden Einstellungen bekannt sein:

- **Serveradresse des SIEM-Systems**

  IP-Adresse des Servers, auf dem das verwendete SIEM-System installiert ist. Dieser Wert muss in den Einstellungen des SIEM-Systems genau bestimmt werden.

- **Serverport des SIEM-Systems**

  Port, über den eine Verbindung zwischen Kaspersky Security Center Cloud Console und dem Server des SIEM-Systems hergestellt wird. Dieser Wert muss in den Einstellungen von Kaspersky Security Center Cloud Console und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

- **Protokoll**

  Das Protokoll, das für die Übertragung von Daten aus Kaspersky Security Center Cloud Console ins SIEM-System verwendet wird. Dieser Wert muss in den Einstellungen von Kaspersky Security Center Cloud Console und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

Über den Ereignisexport

Kaspersky Security Center Cloud Console ermöglicht das automatische Empfangen von Informationen über Ereignisse, die während der Ausführung des Administrationsservers und auf verwalteten Geräten installierter Programme von Kaspersky aufgetreten sind. Die Informationen über Ereignisse werden in der Datenbank des Administrationsservers gespeichert.

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 Apps im Echtzeitbetrieb gewährleisten, sowie Security Operation Center (SOC).

Diese Systeme erhalten Daten aus vielen Quellen, einschließlich Netzwerke, Sicherheitssysteme, Server, Datenbanken und Apps. Ferner gewährleisten SIEM-Systeme eine Zusammenfassung der bearbeiteten Daten, damit Sie keine kritischen Ereignisse überspringen können. Außerdem führen diese Systeme eine automatische Analyse der verbundenen Ereignisse und der Alarme zur Benachrichtigung der Administratoren über Fragen des Sicherheitssystems, die eine sofortige Entscheidung fordern, durch. Die Benachrichtigungen können im Indikatorbereich angezeigt oder über dritte Kanäle, beispielsweise E-Mail, versendet werden.

Am Ablauf des Ereignisexports aus Kaspersky Security Center Cloud Console in die externen SIEM-Systeme sind zwei Seiten beteiligt: der Absender der Ereignisse – Kaspersky Security Center Cloud Console – 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 Security Center Cloud Console angepasst werden. Die Reihenfolge der Einstellungen hat keine Bedeutung: Sie können entweder zuerst den Versand der Ereignisse in der Kaspersky Security Center Cloud Console 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-Apps, 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 Security Center Cloud Console 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 Security Center Cloud Console in die externen SIEM-Systeme sind zwei Seiten beteiligt: der Absender der Ereignisse – Kaspersky Security Center Cloud Console – und der Empfänger der Ereignisse – ein SIEM-System. Der Ereignisexport wird im verwendeten SIEM-System und in der Kaspersky Security Center Cloud Console angepasst.

Die Einstellungen, die im SIEM-System vorgenommen werden, sind vom System abhängig, das Sie verwenden. Im Allgemeinen müssen für alle SIEM-Systeme der Empfänger der Nachrichten und, falls erforderlich, der Nachrichtenparser angepasst werden, damit die erhaltenen Nachrichten auf die Felder verteilt werden können.

Einstellungen des Empfängers der Nachrichten

Für das SIEM-Systems muss der Empfänger für den Erhalt der Ereignisse, die von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console an. Es muss derselbe Port angegeben werden, den Sie als Port in Kaspersky Security Center Cloud Console 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 Security Center Cloud Console empfangen werden, so zu verarbeiten, dass sie in der Datenbank des SIEM-Systems gespeichert werden.

In jedem SIEM-System gibt es einen Satz von Standardparsern für Nachrichten. Kaspersky stellt für einige SIEM-Systeme, beispielsweise QRadar und ArcSight, ebenfalls Nachrichtenparser bereit. Sie können diese Nachrichtenparser von den Webseiten der entsprechenden SIEM-Systeme herunterladen. In den Einstellungen des Empfängers können Sie den verwendeten Nachrichtenparser auswählen: entweder den Standardparser oder den Parser, der von Kaspersky bereitgestellt wird.

Auswählen von Ereignissen für den Export in ein SIEM-System mittels Syslog-Format

Dieser Abschnitt beschreibt das Auswählen von Ereignissen für den weiteren Export in SIEM-Systeme mittels Syslog-Format.

Über das Auswählen von Ereignissen für den Export in SIEM-Systeme mittels Syslog-Format

Nach der Aktivierung des automatischen Ereignisexports müssen Sie markieren, welche Ereignisse in das 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 Programmen auftreten, die von der Richtlinie verwaltet werden. Falls die zu exportierenden Ereignisse in der Richtlinie ausgewählt worden sind, ist es unmöglich, diese für ein einzelnes Programm, das von dieser Richtlinie verwaltet wird, umzudefinieren.

- Ereignisse für ein verwaltetes Programm markieren. Wenn Sie die zu exportierenden Ereignisse für ein verwaltetes Programm auf einem verwalteten Gerät markieren, werden nur Ereignisse in das SIEM-System übertragen, die in diesem Programm aufgetreten sind.

Ereignisse von Kaspersky-Programmen für den Export in das Syslog-Format markieren

Wenn Sie Ereignisse exportieren möchten, die in einem bestimmten verwalteten Programm, welches auf den verwalteten Geräten installiert ist, auftreten, markieren Sie in der Programmrichtlinie 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 ein bestimmtes verwaltetes Programm zu markieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Geräte → Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie des Programms, für welches Sie die Ereignisse markieren möchten.

   Das Fenster mit den Richtlinieneinstellungen wird geöffnet.
3. Wechseln 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 dem verwalteten Programm 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 Programmrichtlinie 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 **Geräte → Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird angezeigt.
2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des benötigten Geräts.

   Das Eigenschaftenfenster des ausgewählten Geräts wird angezeigt.
3. Wechseln Sie zum Abschnitt **Programme**.
4. Klicken Sie in der Liste der Programme auf den Link mit dem Namen des benötigten Programms.
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 für den Export in das Syslog-Format markieren

Sie können allgemeine Ereignisse markieren, die der Administrationsserver unter Verwendung des Syslog-Formats in SIEM-Systeme exportiert.

So markieren Sie Ereignisse für den Export in ein SIEM-System:

1. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).
   - Wechseln Sie im Hauptmenü zu **Geräte** → **Richtlinien und Profile** → und klicken Sie anschließend auf den Link einer Richtlinie.
2. Wechseln Sie im daraufhin geöffneten Fenster auf die Registerkarte **Konfiguration von Ereignissen**.
3. Klicken Sie auf die Schaltfläche **Für den Export in ein SIEM-System mittels Syslog auswählen**.

   Außerdem können Sie im Abschnitt **Ereignisregistrierung**, welcher sich durch Anklicken eines Ereignislinks öffnet, ein Ereignis für den Export in ein SIEM-System markieren.
4. In der Spalte **Syslog** des Ereignisses, oder der Ereignisse, die Sie für den Export in ein SIEM-System markiert haben, erscheint ein Häkchen ( ).

Bei konfiguriertem Export in ein SIEM-System sendet der Administrationsserver ab jetzt die ausgewählten Ereignisse an das SIEM-System.

Über das Exportieren von Ereignissen mittels Syslog-Format

Gemäß dem Syslog-Format können Ereignisse, die auf dem Administrationsserver und in den auf den verwalteten Geräten installierten Programmen von Kaspersky auftreten, ins SIEM-System exportiert werden.

Syslog ist ein Standardprotokoll zur Registrierung von Nachrichten. Dieses Protokoll ermöglicht, die Software, in der die Nachrichten generiert werden, das System, in dem die Nachrichten gespeichert werden, und die Software, in der die Analysen und die Berichterstellung für die Nachrichten ausgeführt wird, zu trennen. Jeder Nachricht wird der Code des Geräts, der den Typ der Software angibt, mit dessen Hilfe die Nachricht erstellt wurde, und die Signifikanz zugewiesen.

Das Syslog-Format wird in den Dokumenten "Request for Comments" (RFC) definiert, die von der Internet Engineering Task Force veröffentlicht werden. Der Standard RFC 5424 wird für den Ereignisexport aus Kaspersky Security Center Cloud Console in externe Systeme verwendet.

In Kaspersky Security Center Cloud Console können Sie den Ereignisexport in externe Systeme gemäß dem Syslog-Format anpassen.

Der Ablauf des Exports besteht aus zwei Schritten:

1. Aktivierung des automatischen Ereignisexports. In diesem Schritt werden die Einstellungen von Kaspersky Security Center Cloud Console so angepasst, dass der Versand von Ereignissen ins SIEM-System ausgeführt werden kann. Der Versand von Ereignissen aus Kaspersky Security Center Cloud Console beginnt sofort nach der Aktivierung des automatischen Exports.

2. Auswahl der Ereignisse, die ins externe System exportiert werden sollen. In diesem Schritt müssen Sie auswählen, welche Ereignisse ins SIEM-System exportiert werden sollen.

Konfiguration von Kaspersky Security Center Cloud Console für den Export an ein SIEM-System

Um Ereignisse an ein SIEM-System zu exportieren müssen Sie den Exportprozess in Kaspersky Security Center Cloud Console konfigurieren.

So konfigurieren Sie den Export in SIEM-Systeme in Kaspersky Security Center Cloud Console:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

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

3. Klicken Sie auf den Link **Einstellungen**.

   Der Abschnitt **Einstellungen exportieren** wird geöffnet.

4. Legen Sie im Abschnitt **Einstellungen exportieren** die Einstellungen fest:

   - **Serveradresse des SIEM-Systems**

     IP-Adresse des Servers, auf dem das verwendete SIEM-System installiert ist. Dieser Wert muss in den Einstellungen des SIEM-Systems genau bestimmt werden.

   - **Port des SIEM-Systems**

     Port, über den eine Verbindung zwischen Kaspersky Security Center Cloud Console und dem Server des SIEM-Systems hergestellt wird. Dieser Wert muss in den Einstellungen von Kaspersky Security Center Cloud Console und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

   - **Protokoll**

Zum Übertragen von Nachrichten an das SIEM-System können Sie ausschließlich das "TLS over TCP"-Protokoll verwenden. Um dies zu tun, müssen Sie die TLS-Einstellungen angeben:

- **Authentifizierung des Servers**

  In dem Feld **Authentifizierung des Servers** können Sie die **Vertrauenswürdige Zertifikate** oder Werte der **SHA-Fingerabdrücke** auswählen:

  - **Vertrauenswürdige Zertifikate**. Sie können eine Datei bekommen, die eine Liste mit Zertifikaten von vertrauenswürdigen Zertifizierungsstellen (Certification Authority – CA) enthält, und diese Datei in Kaspersky Security Center Cloud Console hochladen. Kaspersky Security Center Cloud Console prüft, ob das Zertifikat des SIEM-Servers auch von einer vertrauenswürdigen CA signiert ist oder nicht.

    Um ein vertrauenswürdiges Zertifikat hinzuzufügen, klicken Sie auf die Schaltfläche **CA-Zertifikatsdatei auswählen** und laden Sie anschließend das Zertifikat hoch.

  - **SHA-Fingerabdrücke**. Sie können die SHA-1-Fingerabdrücke der Zertifikate von SIEM-Systemen in Kaspersky Security Center Cloud Console angeben. Um einen SHA-1-Fingerabdruck hinzuzufügen, geben Sie ihn in das Feld **Fingerabdrücke** ein und klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

  Durch Verwendung der Einstellung **Client-Authentifizierung hinzufügen** können Sie ein Zertifikat generieren, um Kaspersky Security Center Cloud Console zu authentifizieren. Infolge dessen verwenden Sie ein selbstsigniertes Zertifikat, das von Kaspersky Security Center Cloud Console ausgestellt wurde. In diesem Fall können Sie sowohl ein vertrauenswürdiges Zertifikat als auch einen SHA-Fingerabdruck verwenden, um den SIEM-Systemserver zu authentifizieren.

- **Name/alternativen Namen des Antragstellers hinzufügen**

  Der Antragstellername ist ein Domänenname, für den das Zertifikat empfangen wird. Kaspersky Security Center Cloud Console kann keine Verbindung zu dem SIEM-System-Server herstellen, wenn der Domänenname des SIEM-System-Servers nicht mit dem Antragstellernamen des Zertifikats des SIEM-System-Servers übereinstimmt. Der SIEM-Systemserver kann jedoch seinen Domänennamen ändern, wenn sich der Name im Zertifikat geändert hat. In diesem Fall können Sie die Antragstellernamen im Feld **Name/alternativen Namen des Antragstellers hinzufügen** angeben. Wenn einer der angegebenen Antragstellernamen mit dem Antragsteller des Zertifikats für das SIEM-Systems übereinstimmt, validiert Kaspersky Security Center Cloud Console das Zertifikat dieses SIEM-Systems.

- **Client-Authentifizierung hinzufügen**

  Um die Client-Authentifizierung durchzuführen, können Sie entweder Ihr Zertifikat einfügen oder es in Kaspersky Security Center Cloud Console generieren.

  - **Zertifikat einfügen**. Sie können ein Zertifikat verwenden, das Sie von einer beliebigen Quelle erhalten haben, beispielsweise von einer vertrauenswürdigen CA. Sie müssen das Zertifikat und seinen privaten Schlüssel angeben, indem Sie einen der folgenden Zertifikat-Typen verwenden:

    - **X.509-Zertifikat PEM**. Laden Sie jeweils eine Datei mit Zertifikat über das Feld **Datei mit Zertifikat** und eine Datei mit privatem Schlüssel über das Feld **Datei mit Schlüssel** hoch. Beide Dateien sind unabhängig voneinander und die Reihenfolge für das Hochladen der Dateien ist spielt keine Rolle. Wenn beide Dateien hochgeladen sind, geben Sie das Kennwort zum Entschlüsseln des privaten Schlüssels in dem Feld **Überprüfung von Kennwort oder Zertifikat** an. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

    - **X.509-Zertifikat PKCS12**. Laden Sie in dem Feld **Datei mit Zertifikat** eine Datei hoch, die ein Zertifikat und dessen privaten Schlüssel enthält. Geben Sie nach dem Hochladen der Datei

das Kennwort zum Entschlüsseln des privaten Schlüssels in dem Feld **Überprüfung von Kennwort oder Zertifikat** an. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

- **Schlüssel generieren**. Sie können in Kaspersky Security Center Cloud Console ein selbstsigniertes Zertifikat generieren. Infolge dessen speichert Kaspersky Security Center Cloud Console das generierte selbstsignierte Zertifikat und Sie können den öffentlichen Teil des Zertifikats oder den SHA1-Fingerabdruck an das SIEM-System übergeben.

5. 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**.

6. Setzen Sie die Option auf die Position **Auto-Exportieren von Ereignissen in die Datenbank des SIEM-Systems Aktiviert**.

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 Datenbank des Administrationsservers ab dem angegebenen Datum gespeichert sind.

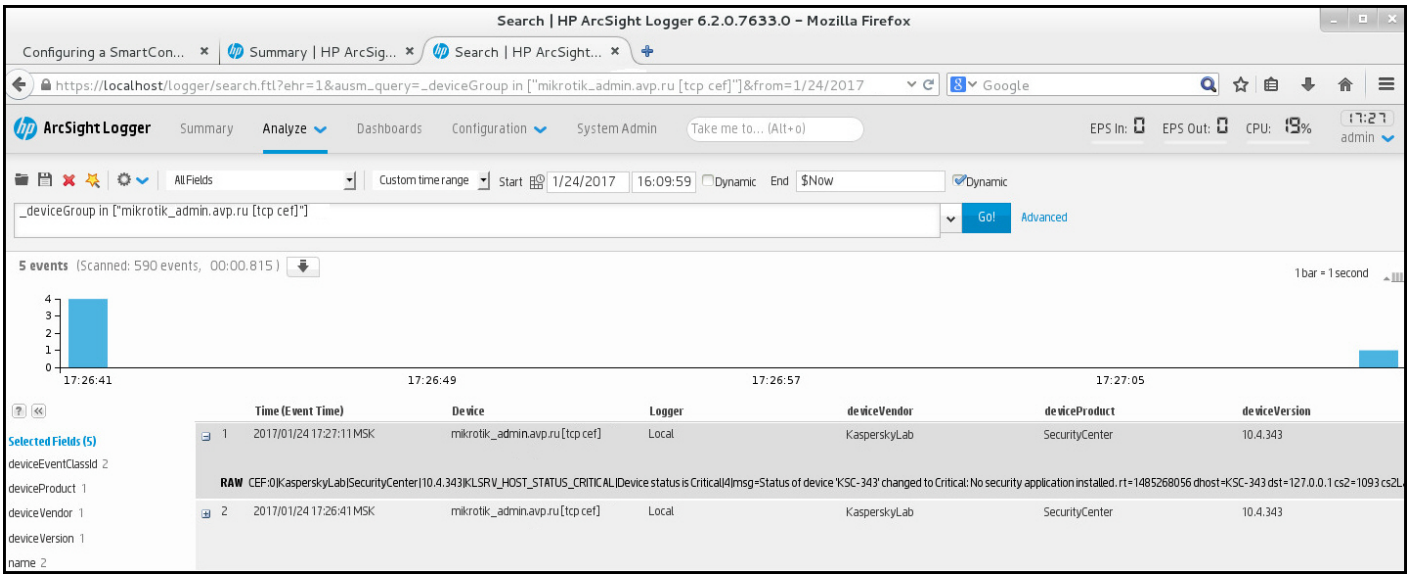
Exportergebnisse anzeigen

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 Security Center Cloud Console versendeten Ereignisse erhalten und vom SIEM-System richtig interpretiert wurden, bedeutet das, dass die Einstellungen auf beiden Seiten korrekt ausgeführt wurden. Andernfalls prüfen Sie und korrigieren Sie erforderlichenfalls die Einstellungen in Kaspersky Security Center Cloud Console 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

Kurzanleitung für Managed Service Provider (MSPs)

Die Kurzanleitung ist für Administratoren von Managed Service Providern (MSPs) gedacht.

Die Kaspersky Security Center Cloud Console 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 Security Center Cloud Console

Kaspersky Security Center Cloud Console ist ein Programm, das von Kaspersky gehostet und verwaltet wird. Sie müssen Kaspersky Security Center Cloud Console nicht auf Ihrem Computer oder Server installieren. Mit Kaspersky Security Center Cloud Console 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 Security Center Cloud Console

Mit Kaspersky Security Center Cloud Console können Sie Folgendes tun:

- Programme von Kaspersky auf Geräten Ihres Netzwerks installieren und die installierten Programme 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-Programmen 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 Security Center Cloud Console als mandantenfähige Anwendung verwenden.
- Kaspersky-Programme, die auf Client-Geräten installiert sind, remote verwalten.
- Die zentrale Bereitstellung von Lizenzschlüsseln für Kaspersky-Programme 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 Security Center Cloud Console für Managed Service Provider (MSPs)

Wenn Sie Kaspersky Security Center Cloud Console starten, können Sie entweder einen Test-Arbeitsbereich auswählen (In diesem Fall erhalten Sie eine 30-tägige Testlizenz, die in Ihrem Arbeitsbereich eingebettet ist), oder den Aktivierungscode einer kommerziellen Lizenz eingeben.

Ein Test-Arbeitsbereich kann nicht in einen kommerziellen umgewandelt werden. Wenn Sie Kaspersky Security Center Cloud Console nach Ablauf der Testlizenz weiterhin verwenden möchten, müssen Sie den Test-Arbeitsbereich löschen und einen neuen Arbeitsbereich mit einer kommerziellen Lizenz anlegen.

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 Security Center Cloud Console kann die Funktionen anderer Kaspersky-Programme in der Benutzeroberfläche der Konsole integrieren. Beispielsweise können Sie Funktionalitäten für Detection and Response zu den Funktionen von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console hinzugefügt (**Überwachung und Berichterstattung** → **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 Security Center Cloud Console hinzugefügt (**Überwachung und Berichterstattung** → **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 Security Center Cloud Console jederzeit ein- oder ausblenden.

Erste Schritte mit Kaspersky Security Center Cloud Console

Wenn Sie das Szenario in diesem Abschnitt abgeschlossen haben, ist Kaspersky Security Center Cloud Console einsatzbereit.

Szenario: Erste Schritte

Das Szenario verläuft in den folgenden Schritten:

1. **Anlegen eines Benutzerkontos**

   Um Kaspersky Security Center Cloud Console zu verwenden, benötigen Sie ein Benutzerkonto.

   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 **Benutzerkonto anlegen**.
   3. Folgen Sie den Anweisungen auf dem Bildschirm.

2. **Anlegen eines Arbeitsbereiches**

   Nachdem Sie ein Benutzerkonto angelegt haben, können Sie Ihr Unternehmen registrieren und Ihren Arbeitsbereich erstellen.

   Wenn Sie Kaspersky Security Center Cloud Console starten, können Sie entweder einen Test-Arbeitsbereich auswählen (In diesem Fall erhalten Sie eine 30-tägige Testlizenz, die in Ihrem Arbeitsbereich eingebettet ist), oder den Aktivierungscode einer kommerziellen Lizenz eingeben.

Ein Test-Arbeitsbereich kann nicht in einen kommerziellen umgewandelt werden. Wenn Sie Kaspersky Security Center Cloud Console nach Ablauf der Testlizenz weiterhin verwenden möchten, müssen Sie den Test-Arbeitsbereich löschen und einen neuen Arbeitsbereich mit einer kommerziellen Lizenz anlegen.

So registrieren Sie ein Unternehmen und legen 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 Security Center Cloud Console**

   Wenn Sie den erstellten Arbeitsbereich zum ersten Mal öffnen, werden Sie automatisch dazu aufgefordert, den Schnellstartassistenten auszuführen. Der Schnellstartassistenten 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-Programme. Folgen Sie den Anweisungen auf dem Bildschirm.

Wenn die Erstkonfiguration abgeschlossen wurde, ist Kaspersky Security Center Cloud Console 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 Security Center Cloud Console migrieren.

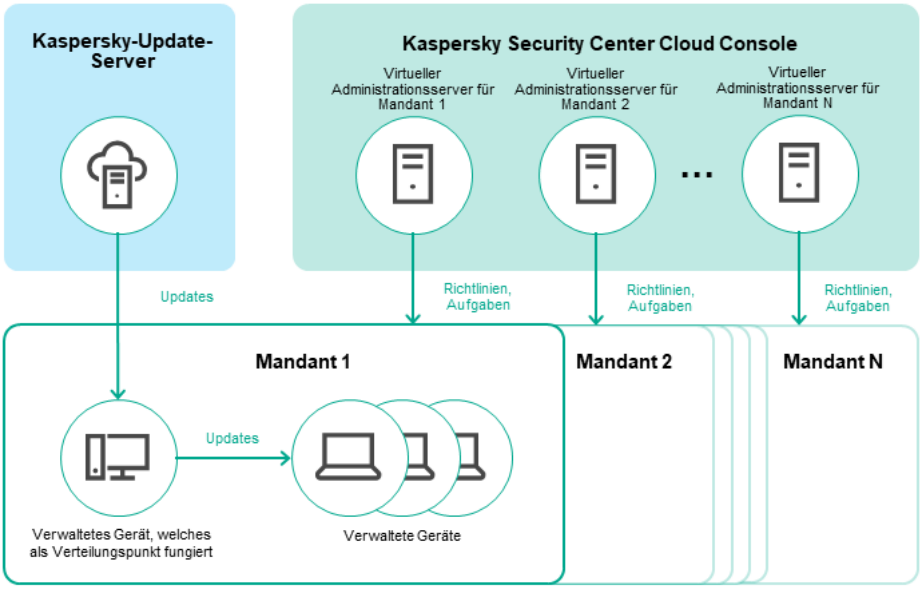
  Virtuelle Administrationsserver können nicht migriert werden. Nach der Migration der Administrationsgruppen und anderer Objekte können Sie in der Kaspersky Security Center Cloud Console virtuelle Administrationsserver erstellen.

  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 Security Center Cloud Console*. Stellt eine Benutzeroberfläche für die Verwaltungsdienste Ihres Arbeitsbereichs zur Verfügung. Sie verwenden die Komponente von Kaspersky Security Center Cloud Console, um das Schutzsystem für das Netzwerk eines Kundenunternehmens bereitzustellen, zu verwalten und zu warten.

- *Kaspersky-Update-Server*. HTTP(S)-Server bei Kaspersky, von denen Programme von Kaspersky Updates für Datenbanken und Programm-Module herunterladen.

- *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 Security Center Cloud Console 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 ihnen manuell Verteilungspunkte zu.

Szenario: Bereitstellung des Schutzes (Verwaltung von Mandanten mittels virtueller Administrationsserver)

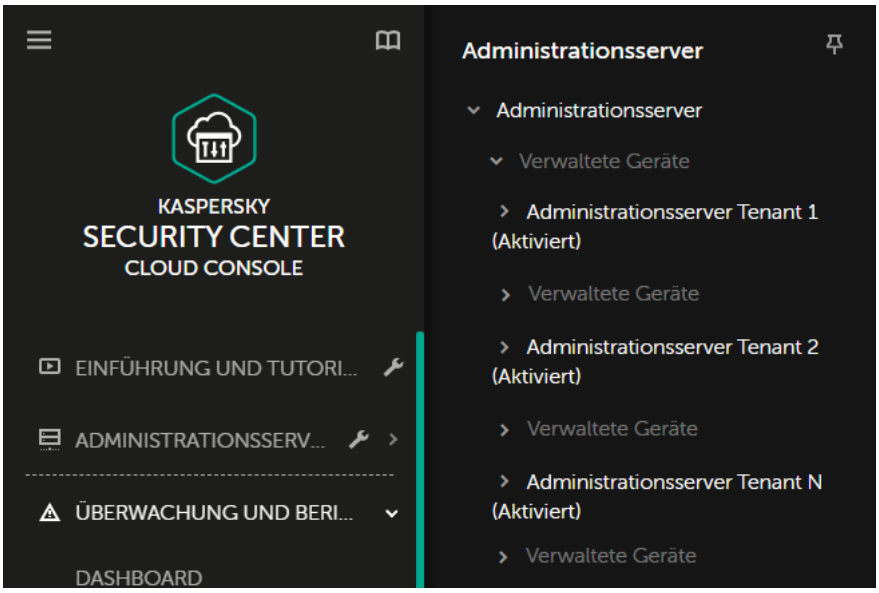
Wenn Sie Kaspersky Security Center noch nie verwendet haben und Sie Ihre Mandanten über virtuelle Administrationsserver verwalten möchten, gehen Sie wie in diesem Abschnitt beschrieben vor. Wenn Sie das Szenario abgeschlossen haben, werden die Geräte Ihrer Kunden geschützt.

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 Security Center Cloud Console 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-Programme erstellen**

   Erstellen Sie Installationspakete für Kaspersky-Programme.

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-Programmen.

10. **Kaspersky-Programme auf Client-Geräten installieren**

    Erstellen Sie Aufgaben zur Remote-Installation, um den Administrationsagenten und verwaltete Kaspersky-Programme auf Ihren Kundengeräten zu installieren.

    Wenn benötigt, können Sie auch mehrere Aufgaben zur Remote-Installation zum Installieren von verwalteten Kaspersky-Programmen 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-Programmen ausgeführt werden.

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

    Lassen Sie sich den **Bericht über Versionen der Kaspersky-Programme** generieren und anzeigen. Stellen Sie sicher, dass die verwalteten Kaspersky-Programme auf allen Geräten Ihres Kunden installiert sind.

12. **Erstellen von Richtlinien für Kaspersky-Programme**

    Erstellen Sie eine Richtlinie für das benötigte Kaspersky-Programm. 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 das gewünschte Kaspersky-Programm.

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 Security Center Cloud Console 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-Programme.

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-Programmen.

10. **Installieren von Kaspersky-Programmen auf den Geräten Ihrer Kunden**

    Erstellen Sie Aufgaben zur Remote-Installation, um den Administrationsagenten und verwaltete Kaspersky-Programme auf Ihren Kundengeräten zu installieren.

    Wenn benötigt, können Sie auch mehrere Aufgaben zur Remote-Installation zum Installieren von verwalteten Kaspersky-Programmen 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-Programmen ausgeführt werden.

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

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

12. **Erstellen von Richtlinien für Kaspersky-Programme**

    Rufen Sie das Menü **Geräte → 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 das benötigte Kaspersky-Programm.

Gemeinsame Verwendung von einem lokal ausgeführten Kaspersky Security Center und Kaspersky Security Center Cloud Console

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 Security Center Cloud Console konvertieren, wie in diesem Abschnitt beschrieben.

Wenn Sie die gemeinsame Verwendung von einem lokal ausgeführten Kaspersky Security Center und Kaspersky Security Center Cloud Console konfigurieren, können Sie nur dann von einem lokalen Kaspersky Security Center auf Kaspersky Security Center Cloud Console 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 Security Center Cloud Console ermöglicht eine zentrale Verteilung von Lizenzschlüsseln für Kaspersky-Programme 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 Security Center Cloud Console 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-Programme sind aktiviert.

Überwachungs- und Berichtsfunktionen für Managed Service Provider (MSPs)

Kaspersky Security Center Cloud Console 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.

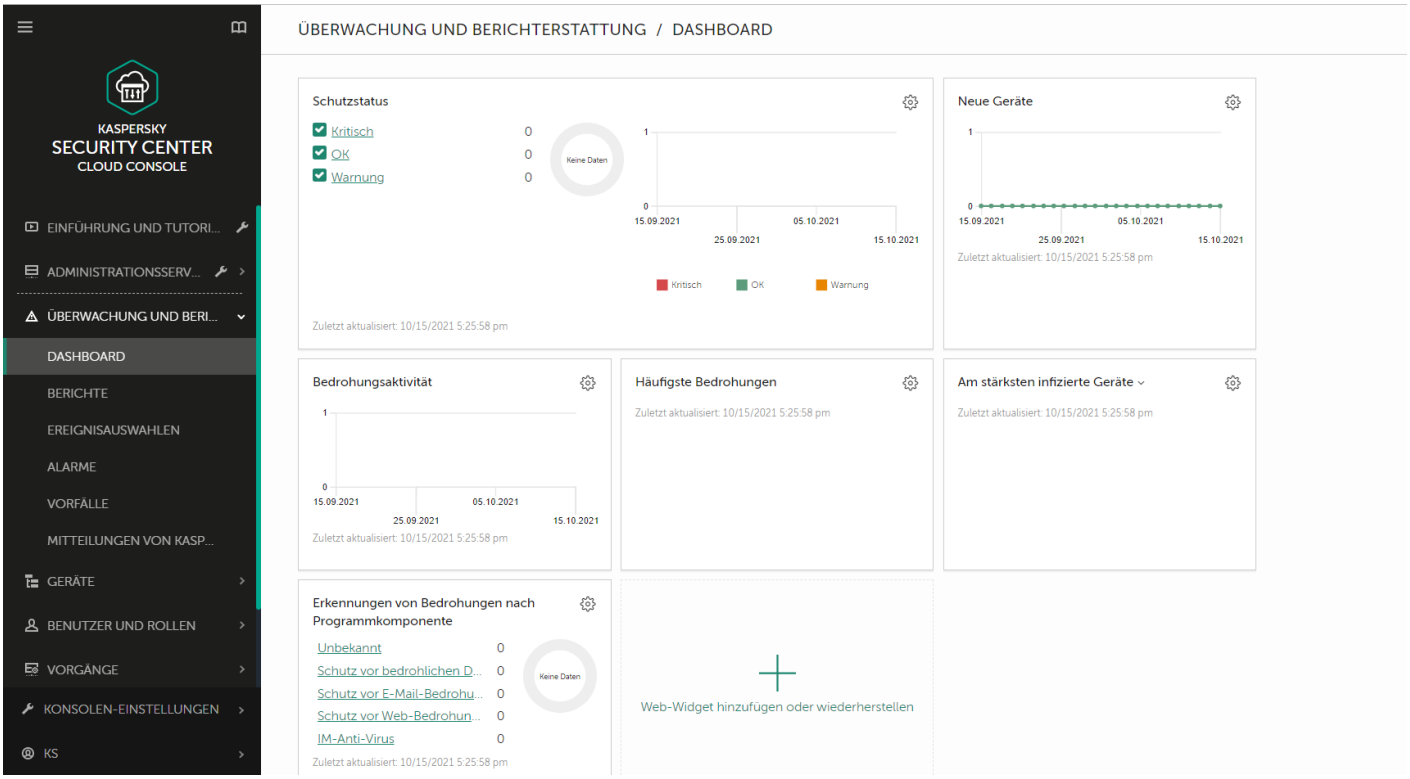
Wenn Sie Kaspersky Security Center Cloud Console bereitgestellt haben, können Sie die Funktionen zur Überwachung und Berichterstattung konfigurieren, um sie an Ihre Bedürfnisse anzupassen.

Kaspersky Security Center Cloud Console stellt die folgenden Funktionen zur Überwachung und Berichterstattung zur Verfügung:

- Dashboard
- Berichte
- Ereignisauswahlen
- E-Mail-Benachrichtigungen

Dashboard

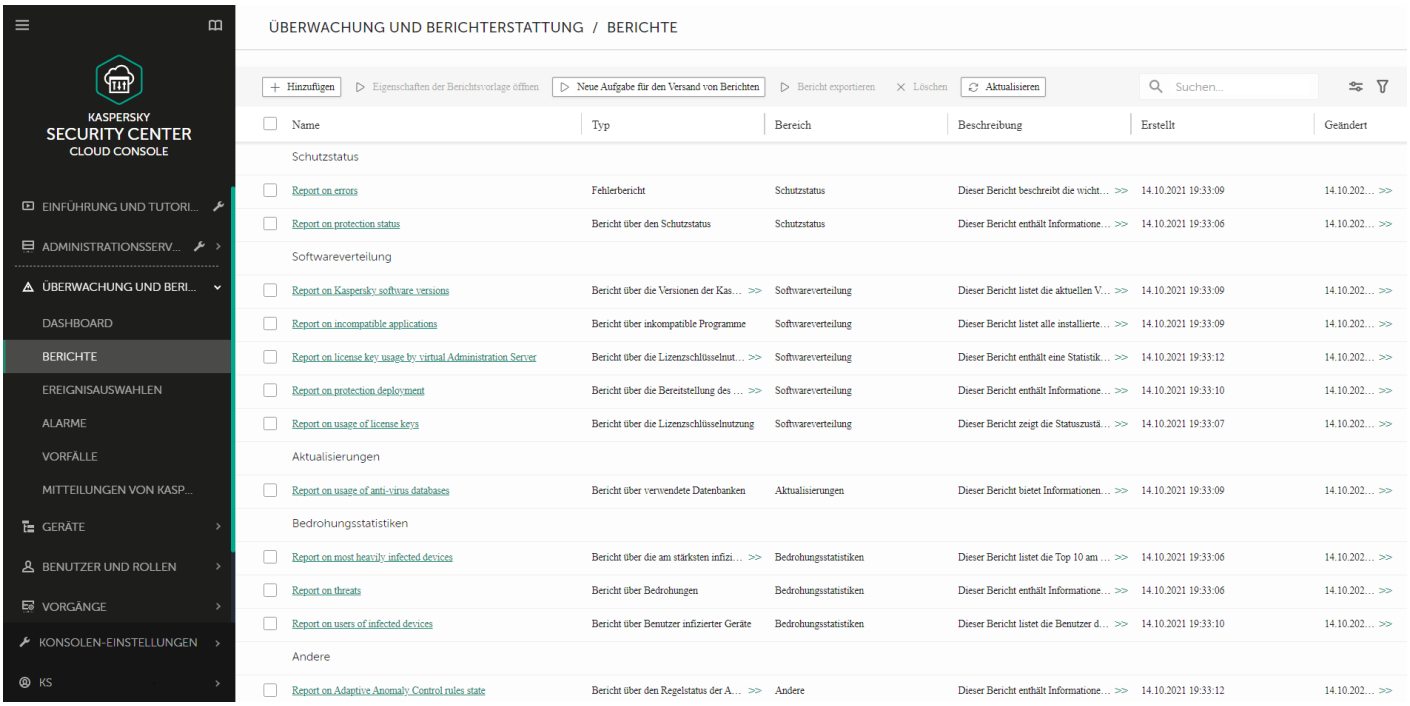
Das Dashboard bietet eine grafische Darstellung von Informationen und erlaubt Ihnen, sicherheitsrelevante Entwicklungen in Ihrem Unternehmensnetzwerk zu überwachen (Siehe Abbildung unten).



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 Security Center Cloud Console 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 Security Center Cloud Console und auf Ihren Kundengeräten auftreten, informiert zu werden.

Arbeiten mit Kaspersky Security Center Cloud Console in einer Cloud-Umgebung

Dieser Abschnitt bietet Informationen zu Kaspersky Security Center Cloud Console in Bezug auf den Betrieb und die Wartung von Kaspersky Security Center Cloud Console 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.

Varianten der Lizenzierung in der Cloud-Umgebung

Das Arbeiten in einer Cloud-Umgebung ist sowohl im Testmodus als auch kommerziellen Modus der Kaspersky Security Center Cloud Console 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 Sie versuchen, die Funktion zur Arbeit in der Cloud-Umgebung mit einer Lizenz für Kaspersky Hybrid Cloud Security zu aktivieren, kann ein Fehler auftreten.

Vorbereitung auf das Arbeiten in einer Cloud-Umgebung mittels Kaspersky Security Center Cloud Console

In diesem Abschnitt erfahren Sie, wie Sie sich für die Arbeit mit Kaspersky Security Center Cloud Console 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 Security Center Cloud Console in Amazon Web Services vorbereiten.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console 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 anschließen Kaspersky Security für Windows Server und Kaspersky Endpoint Security für Linux zu installieren.

Sicherstellen der Berechtigungen zur Arbeit der Kaspersky Security Center Cloud Console mit AWS

Um in der Cloud-Umgebung von Amazon Web Services mit Kaspersky Security Center Cloud Console zu arbeiten, müssen Sie ein *IAM-Benutzerkonto* erstellen, welches von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console

Für die Arbeit mit der Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console aktuell.

Arbeiten mit der Cloud-Umgebung Microsoft Azure

Dieser Abschnitt informiert über den Betrieb und die Wartung von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console arbeiten.

Erstellen eines Abonnements, einer Anwendungs-ID und eines Kennworts

Zum Arbeiten mit Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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+QIfFvdU=). Die Beschreibung wird wie von Ihnen eingegeben angezeigt.
6. Kopieren Sie das Kennwort und bewahren Sie es auf, um es Kaspersky Security Center Cloud Console später zusammen mit der Anwendungs-ID bereitzustellen.

   Sie können das Kennwort nur nach seiner Erstellung kopieren. Zu einem späteren Zeitpunkt wird das Kennwort nicht mehr angezeigt und kann nicht wiederhergestellt werden.

Die in diesem Dokument zitierten Webadressen waren zum Zeitpunkt des Veröffentlichungsdatums von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console in einer von Google bereitgestellten Cloud-Umgebung.

Sie können die Google API verwenden, um mit Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console

Um Kaspersky Security Center Cloud Console 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 Server

Der Assistent für das Konfigurieren der Cloud-Umgebung wird bei der ersten Verbindung mit Kaspersky Security Center Cloud Console automatisch gestartet, wenn Ihr Arbeitsbereich mithilfe der Lizenz für Kaspersky Hybrid Cloud Security erstellt wurde. 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 Softwareverteilung → Softwareverteilung und Zuweisung → Konfigurieren der Cloud-Umgebung**.

Der Assistent wird gestartet.

Eine durchschnittliche Arbeitssitzung mit diesem Assistenten dauert etwa 15 Minuten.

Schritt 1. Überprüfen der erforderlichen Plug-ins und Installationspakete

Dieser Schritt wird nicht angezeigt, wenn Sie bereits über alle unten aufgeführten erforderlichen Web-Plug-Ins und Installationspakete verfügen.

Um eine Cloud-Umgebung zu konfigurieren, benötigen Sie die folgenden Komponenten:

- Installationspakete:
    - Administrationsagent für Windows
    - Administrationsagent für Linux
    - Kaspersky Endpoint Security für Linux
- Web-Plug-in für Kaspersky Endpoint Security für Linux
- Mindestens eines der folgenden:
    - Installationspaket und Web-Plug-in für Kaspersky Endpoint Security für Windows (empfohlen)
    - Installationspaket und Web-Plug-in für Kaspersky Security für Windows Server

Wir empfehlen Ihnen, Kaspersky Endpoint Security für Windows anstelle von Kaspersky Security für Windows Server zu verwenden.

Kaspersky Security Center Cloud Console 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 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".

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:

- **Anwendungs-ID für Azure**

  Sie haben diese Anwendungs-ID auf dem Azure-Portal erstellt.

  Sie können nur eine Azure Anwendungs-ID für Abfragen und andere Zwecke bereitstellen. Wenn Sie ein anderes Azure-Segment abfragen möchten, müssen Sie zunächst die bestehende Azure-Verbindung löschen.

- **Azure-Abonnement-ID**

  Sie haben das Abonnement auf dem Azure-Portal erstellt.

- **Azure-App-Kennwort**

  Sie haben das Kennwort zur Anwendungs-ID bei der Erstellung der Anwendungs-ID erhalten.

  Die Zeichen des Kennworts werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des Kennworts begonnen haben, wird die Schaltfläche **Anzeigen** eingeblendet. Klicken Sie auf diese Schaltfläche und halten Sie diese gedrückt, um die eingegebenen Zeichen anzuzeigen.

  Um die von Ihnen eingegebenen Zeichen anzuzeigen, klicken Sie die Schaltfläche **Anzeigen** und halten Sie diese gedrückt.

- **Name des Azure-Speicherkontos**

Der Name des Azure-Speicherkontos, das Sie erstellt haben, um mit Kaspersky Security Center Cloud Console zu arbeiten.

- **Zugriffsschlüssel für Azure-Speicher**

  Sie haben das Kennwort (den Schlüssel) erhalten, als Sie das Azure-Speicherkonto für die Verwendung von Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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. Auswählen der Anwendung, für die eine Richtlinie und Aufgaben erstellt werden sollen

Dieser Schritt wird nur angezeigt, wenn Sie über Installationspakete und Plug-ins sowohl für Kaspersky Endpoint Security für Windows als auch für Kaspersky Security für Windows Server verfügen. Wenn Sie nur für eines dieser Programme über ein Plug-in und ein Installationspaket verfügen, wird dieser Schritt übersprungen und die Kaspersky Security Center Cloud Console erstellt eine Richtlinie und Aufgaben für das vorhandene Programm.

Wählen Sie ein Programm aus, für das Sie eine Richtlinie und Aufgaben erstellen möchten:

- Kaspersky Endpoint Security für Windows
- Kaspersky Security für Windows Server

Schritt 6. Konfiguration von Kaspersky Security Network für Kaspersky Security Center Cloud Console

Dieser Schritt wird übersprungen, wenn Sie Kaspersky Security Center Cloud Console im Testmodus oder auf einem virtuellen Administrationsserver ausführen.

Legen Sie die Einstellungen für das Übertragen von Informationen über die Ausführung von Kaspersky Security Center Cloud Console in die Wissensdatenbank von Kaspersky Security Network (KSN) fest. Wählen Sie eine der folgenden Varianten aus:

- **Ich akzeptiere die Nutzungsbedingungen für Kaspersky Security Network**

  Kaspersky Security Center Cloud Console 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 Nutzungsbedingungen für Kaspersky Security Network ab**

  Kaspersky Security Center Cloud Console und verwaltete Programme senden keine Informationen an Kaspersky Security Network.

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

Kaspersky empfiehlt die Teilnahme an Kaspersky Security Network.

Die KSN-Erklärungen verwalteter Programme können ebenfalls angezeigt werden. Wenn Sie die Nutzungsbedingungen von Kaspersky Security Network akzeptieren, überträgt das verwaltete Programm Daten an Kaspersky. Wenn Sie der Teilnahme an Kaspersky Security Network nicht zustimmen, überträgt das verwaltete Programm keine Daten an Kaspersky. Sie können diese Einstellung später in der Programmrichtlinie ändern.

Klicken Sie auf **Weiter** um fortfahren.

Schritt 7. Erstellen einer Erstkonfiguration des Schutzes

Sie können die Liste mit Richtlinien und Aufgaben, die erstellt werden, überprüfen.

Warten Sie, bis die Erstellung der Richtlinien und Aufgaben abgeschlossen ist, und klicken Sie auf **Weiter**, um fortzufahren. Klicken Sie auf der Letzten Seite des Assistenten auf **Fertigstellen**, um ihn zu verlassen.

Abfrage von Netzwerksegmenten mittels Kaspersky Security Center Cloud Console

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 Security Center Cloud Console 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 Security Center Cloud Console

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 Softwareverteilung** → **Entdeckung** → **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:

  - **Anwendungs-ID für Azure**

    Sie haben diese Anwendungs-ID auf dem Azure-Portal erstellt.

    Sie können nur eine Azure Anwendungs-ID für Abfragen und andere Zwecke bereitstellen. Wenn Sie ein anderes Azure-Segment abfragen möchten, müssen Sie zunächst die bestehende Azure-Verbindung löschen.

  - **Azure-Abonnement-ID**

    Sie haben das Abonnement auf dem Azure-Portal erstellt.

  - **Azure-App-Kennwort**

    Sie haben das Kennwort zur Anwendungs-ID bei der Erstellung der Anwendungs-ID erhalten.

    Die Zeichen des Kennworts werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des Kennworts begonnen haben, wird die Schaltfläche **Anzeigen** eingeblendet. Klicken Sie auf diese Schaltfläche und halten Sie diese gedrückt, um die eingegebenen Zeichen anzuzeigen.

    Um die von Ihnen eingegebenen Zeichen anzuzeigen, klicken Sie die Schaltfläche **Anzeigen** und halten Sie diese gedrückt.

  - **Name des Azure-Speicherkontos**

    Der Name des Azure-Speicherkontos, das Sie erstellt haben, um mit Kaspersky Security Center Cloud Console zu arbeiten.

  - **Zugriffsschlüssel für Azure-Speicher**

    Sie haben das Kennwort (den Schlüssel) erhalten, als Sie das Azure-Speicherkonto für die Verwendung von Kaspersky Security Center Cloud Console 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 Softwareverteilung → Entdeckung → 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 Security Center Cloud Console 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 Softwareverteilung** → **Entdeckung** → **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 (Min.)**

  Geben Sie an, wofür n steht (Minuten oder Tage).

- **Beginnend ab**

  Geben Sie an, wann mit der ersten Abfrage begonnen werden soll.

- **Übersprungene Aufgaben starten**

  Wenn Ihr Arbeitsbereich während der für die Abfrage geplanten Zeit nicht verfügbar ist, kann Kaspersky Security Center Cloud Console die Abfrage entweder sofort starten, nachdem er wieder verfügbar ist, oder auf die nächste planmäßige Durchführung warten.

  Wenn diese Option aktiviert ist, beginnt Kaspersky Security Center Cloud Console sofort mit der Abfrage, nachdem der Arbeitsbereich wieder verfügbar ist.

  Wenn diese Option deaktiviert ist, wartet Kaspersky Security Center Cloud Console 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 Security Center Cloud Console

Sie können die Ergebnisse der Abfrage des Cloud-Segments, d. h. die Liste der vom Administrationsserver verwalteten Cloud-Geräte, anzeigen.

Um die Ergebnisse der Abfrage des Cloud-Segments anzuzeigen, gehen Sie wie folgt vor:

Wechseln Sie im Hauptmenü zu **Gerätesuche und Softwareverteilung → Entdeckung → Cloud**.

Die für die Abfrage verfügbaren Cloud-Segmente werden angezeigt.

Anzeigen der Eigenschaften von Cloud-Geräten mittels Kaspersky Security Center Cloud Console

Sie können die Eigenschaften jedes Cloud-Geräts anzeigen.

Um die Eigenschaften eines Cloud-Gerätes anzuzeigen:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte**.
2. Klicken Sie auf den Namen des Geräts, dessen Eigenschaften Sie anzeigen möchten.

   Es wird Eigenschaftenfenster geöffnet, in dem der Abschnitt **Allgemein** ausgewählt ist.
3. Wenn Sie speziell die Eigenschaften für Cloud-Geräte anzeigen wollen, wählen Sie im Eigenschaftenfenster den Abschnitt **System** aus.

   Die angezeigten Eigenschaften sind abhängig von der Cloud-Plattform des Geräts.

   Für Geräte in AWS werden die folgenden Eigenschaften angezeigt:

   - **Gefunden mithilfe von API** (Wert: **AWS**)
   - **Cloud-Region**
   - **Cloud-VPC**
   - **Cloud Availability Zone (Verfügbarkeitszone)**
   - **Cloud-Subnetz**
   - **Cloud-Placement-Gruppe** (Dieses Element wird nur angezeigt, wenn die Instance zu einer Platzierungsgruppe gehört - andernfalls wird es nicht angezeigt)

   Für Geräte in Azure werden die folgenden Eigenschaften angezeigt:

   - **Gefunden mithilfe von API** (Wert: **Microsoft Azure**)
   - **Cloud-Region**
   - **Cloud-Subnetz**

   Für Geräte in Google Cloud werden die folgenden Eigenschaften angezeigt:

   - **Gefunden mithilfe von API** (Wert: **Google Cloud**)
   - **Cloud-Region**
   - **Cloud-VPC**
   - **Cloud Availability Zone (Verfügbarkeitszone)**
   - **Cloud-Subnetz**

Synchronisation mit der Cloud: Konfigurieren der Verschiebungsregel

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 Softwareverteilung** → **Softwareverteilung 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 Security Center Cloud Console erstellt. Wird zum Beispiel ein neues Subnetz während der Gerätesuche gefunden, wird eine neue Gruppe mit dem gleichen Namen in der Gruppe **Verwaltete Geräte\Cloud** erstellt.

     Wenn diese Option deaktiviert ist, erstellt Kaspersky Security Center Cloud Console 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 Security Center Cloud Console 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 Security Center Cloud Console unterstützt die folgenden Szenarien:

- Ein Client-Gerät wird mittels der Azure-API gefunden; die Installation erfolgt ebenfalls mittels einer API. Wenn Sie die Azure-API verwenden, können Sie nur die folgenden Programme installieren:
  - Kaspersky Endpoint Security für Linux

- Kaspersky Endpoint Security für Windows
- Kaspersky Security für Windows Server

- Ein Client-Gerät wird mittels der Azure-API gefunden; die Installation wird unter Verwendung von Verteilungspunkten durchgeführt oder – wenn dieser nicht zur Verfügung steht – manuell mittels Standalone-Installationspaketen. Mit dieser Methode können Sie alle Programme installieren, die von Kaspersky Security Center Cloud Console unterstützt werden.

So erstellen Sie eine Aufgabe zur Remote-Installation eines Programms auf virtuellen Maschinen von Azure:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Folgen Sie den Anweisungen des Assistenten:

   a. Wählen Sie den Aufgabentyp **Remote-Installation eines Programms** aus.

   b. Wählen Sie auf der Seite **Installationspakete** die Option **Remote-Installation mittels API von Microsoft Azure**.

   c. Geben Sie bei der Auswahl des Kontos für den Zugriff auf Geräte ein vorhandenes Azure-Konto an oder klicken Sie auf **Hinzufügen** und geben Sie die Anmeldeinformationen Ihres Azure-Kontos ein:

   - **Azure-Kontoname**

     Geben Sie einen beliebigen Namen für die von Ihnen angegebenen Anmeldeinformationen ein. Dieser Name wird in der Liste der Benutzerkonten zur Ausführung der Aufgabe angezeigt.

   - **Anwendungs-ID für Azure**

     Sie haben diese Anwendungs-ID auf dem Azure-Portal erstellt.

     Sie können nur eine Azure Anwendungs-ID für Abfragen und andere Zwecke bereitstellen. Wenn Sie ein anderes Azure-Segment abfragen möchten, müssen Sie zunächst die bestehende Azure-Verbindung löschen.

   - **Azure-App-Kennwort**

     Sie haben das Kennwort zur Anwendungs-ID bei der Erstellung der Anwendungs-ID erhalten.

     Die Zeichen des Kennworts werden in Form von Sternchen angezeigt. Nachdem Sie mit der Eingabe des Kennworts begonnen haben, wird die Schaltfläche **Anzeigen** eingeblendet. Klicken Sie auf diese Schaltfläche und halten Sie diese gedrückt, um die eingegebenen Zeichen anzuzeigen.

   d. Wählen Sie die notwendigen Geräte aus der Gruppe **Verwaltete Geräte\Cloud** aus.

Nachdem der Assistent abgeschlossen ist, wird die Aufgabe zur Remote-Installation des Programms in der Aufgabenliste angezeigt.

Sprache der Benutzeroberfläche von Kaspersky Security Center Cloud Console ändern

Sie können die Sprache der Benutzeroberfläche von Kaspersky Security Center Cloud Console auswählen.

So ändern Sie die Sprache der Benutzeroberfläche:

1. Wechseln Sie im Hauptmenü zu **Konsolen-Einstellungen** → **Sprache**.
2. Wählen Sie eine der unterstützten Lokalisierungssprachen aus.

Anfrage an den Technischen Support

Dieser Abschnitt beschreibt, wie Sie technischen Support erhalten können, und nennt die dafür notwendigen Voraussetzungen.

Wie Sie technischen Support erhalten können

Wenn Sie weder in der Dokumentation von Kaspersky Security Center Cloud Console noch in den anderen Informationsquellen zu Kaspersky Security Center Cloud Console keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support von Kaspersky. Die Mitarbeiter des Technischen Supports beantworten alle Fragen zur Installation und Verwendung von Kaspersky Security Center Cloud Console.

Kaspersky bietet die Unterstützung für Kaspersky Security Center Cloud Console im Rahmen dessen Lebenszyklus' an (siehe Seite mit dem Produktlebenszyklus). 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 Seite des Technischen Supports
- Versand einer Anfrage an den Technischen Support aus dem Portal Kaspersky CompanyAccount

Technischer Support über Kaspersky CompanyAccount

Kaspersky CompanyAccount ist ein Portal für Unternehmen, die Kaspersky-Programme verwenden. Das Portal Kaspersky CompanyAccount dient der Kontaktaufnahme mit den Spezialisten von Kaspersky über elektronische Anfragen. Sie können Kaspersky CompanyAccount verwenden, um den Status Ihrer Online-Anfragen zu verfolgen sowie deren Verlauf zu speichern.

Sie können alle Mitarbeiter Ihrer Firma unter einem Benutzerkonto für Kaspersky CompanyAccount registrieren. Mithilfe eines einheitlichen Benutzerkontos 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 Website 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 Security Center Cloud Console
- ID des Arbeitsbereichs
- Lizenzinformation
- Anzahl der installierten Programme
- Mandanten-ID und -Status

Diese Informationen befinden sich im Abschnitt **Ihr Benutzerkonto** →**Technischer Support**. Kopieren Sie die Informationen und leiten Sie diese weiter, um Unterstützung bei Ihrem Problem zu bekommen.

Informationsquellen über das Programm

Seite von Kaspersky Security Center Cloud Console auf der Website von Kaspersky

In dem Abschnitt zu Kaspersky Security Center Cloud Console auf der Kaspersky-Website finden Sie allgemeine Informationen über die Anwendung, ihre Funktionen und Besonderheiten.

Seite von Kaspersky Security Center Cloud Console in der Wissensdatenbank

Die *Wissensdatenbank* ist ein Abschnitt der Website des Technischen Supports von Kaspersky.

In dem Abschnitt von Kaspersky Security Center Cloud Console in der Wissensdatenbank finden Sie Artikel mit nützlichen Informationen, Tipps und Antworten auf häufige Fragen zu Erwerb, Installation und Nutzung des Programms.

Neben Fragen zu Kaspersky Security Center Cloud Console können die Artikel auch andere Programme von Kaspersky betreffen. Artikel in der Wissensdatenbank können auch Neuigkeiten über den Technischen Support enthalten.

In der Community über Anwendungen von Kaspersky 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 Security Center Cloud Console hat eine Reihe von Einschränkungen, die für die Verwendung des Programms nicht kritisch sind:

- Für Verteilungspunkte, die als Push-Server fungieren, funktioniert die in den Richtlinieneinstellungen des Administrationsagenten enthaltene Option **Ports des Administrationsagenten in der Windows-Firewall öffnen** nicht ordnungsgemäß. Wenn Sie einen Verteilungspunkt als Push-Server verwenden, müssen Sie den Port des Push-Servers manuell zur Ausschlussliste der Microsoft Windows-Firewall hinzufügen, um eine Verbindung zwischen dem Push-Server und einem verwalteten Gerät herzustellen.

- Wenn Sie in den Richtlinieneinstellungen von Kaspersky Security für mobile Endgeräte in einem Abschnitt einige Einstellungen angeben und anschließend zu einem anderen Abschnitt wechseln, ohne die Änderungen vorher zu speichern, werden diese Änderungen nicht übernommen.

- Wenn Sie im Browser Mozilla Firefox ein Video aus dem Abschnitt **Einführung und 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.

- Wenn Sie für die Option **Speicherdauer für die Revisionen von Objektänderungen (Tage)** den Standardwert ändern, wird dieser Wert in der Ereignisbeschreibung als "Nichts" angezeigt.

- Wenn Sie versuchen, sich mit Active Directory Federation Services (ADFS) an der Kaspersky Security Center Cloud Console anzumelden, aber die erforderlichen Berechtigungen fehlen, gibt die Kaspersky Security Center Cloud Console immer noch den Fehler "Ungültige Anmeldedaten" zurück, anstatt den Benutzer über fehlende Berechtigungen zu warnen.

- Wenn Sie die Breite der Spalte **Name** im Abschnitt **Gerätesuche und Softwareverteilung → Softwareverteilung und Zuweisung → Installationspakete** vergrößern, schlägt das Vergrößern der Spalte fehl, und die Breite der Spalte wird stattdessen auf ihren Standardwert zurückgesetzt.

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

- 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.

- 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.

Glossar

Administrationsagent

Eine Komponente von Kaspersky Security Center Cloud Console, mit deren Hilfe die Interaktion zwischen dem Administrationsserver und den Programmen von Kaspersky 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 Programme von Kaspersky, 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 Programmen von Kaspersky gruppiert sind. Geräte sind zur erleichterten Verwaltung als einzelne Entität gruppiert. Eine Gruppe kann andere Gruppen beinhalten. Für jedes installierte Programm in der Gruppe können Gruppenrichtlinien und Gruppenaufgaben erstellt werden.

Administrationsserver

Eine Komponente von Kaspersky Security Center Cloud Console, die Informationen über alle Programme von Kaspersky, die innerhalb des Unternehmensnetzwerks installiert sind, zentral speichert. Sie kann auch zur Verwaltung dieser Programme verwendet werden.

Aktiver Schlüssel

Ein Schlüssel, der momentan vom Programm 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 Security Center Cloud Console, 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 ein Programm von Kaspersky 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 Security Center Cloud Console 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.

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

Programmverwaltung über eine lokale Schnittstelle.

Ereignis-Datenverwaltung

Ein Teil der Datenbank des Administrationsservers, der Speicherung von Informationen über Ereignisse im Kaspersky Security Center Cloud Console 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-Programmen, 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 der auf BIOS-Ebene integrierten Software Kaspersky Anti-Virus für UEFI. 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 des Programms 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-Programm eines fremden Entwicklers oder Programm von Kaspersky, das die Verwaltung über Kaspersky Security Center Cloud Console nicht unterstützt.

Installationspaket

Ein Satz von Dateien, der für die Remote-Installation einer Kaspersky-Anwendung mithilfe des Remote-Verwaltungssystems von Kaspersky Security Center Cloud Console 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 Private Security Network (KPSN)

Die Lösung Kaspersky Private Security Network gewährt Benutzern von Geräten, auf denen Programme von Kaspersky installiert sind, Zugriff auf die Reputationsdatenbanken von Kaspersky Security Network sowie auf andere statistische Daten, ohne dass Daten von ihren Geräten an Kaspersky Security Network gesendet werden müssen. Kaspersky Private Security Network richtet sich an Unternehmenskunden, die aus einem der folgenden Gründe nicht an Kaspersky Security Network teilnehmen können:

- Die Geräte haben keine Internetverbindung.
- Die Übermittlung von Daten an einen Punkt außerhalb des Landes oder des lokalen Unternehmensnetzwerks ist gesetzlich oder aufgrund von Sicherheitsrichtlinien des Unternehmens untersagt.

Kaspersky Security Center Cloud Console Administrator

Person, die Programmvorgänge über das zentralisierte Remote-Verwaltungssystem Kaspersky Security Center Cloud Console verwaltet.

Kaspersky Security Center Cloud Console Operator

Benutzer, der den Status und Betrieb eines Schutzsystems überwacht, das mithilfe von Kaspersky Security Center Cloud Console verwaltet wird.

Kaspersky Security Network (KSN)

Infrastruktur der Cloud-Dienste, die den umfassenden Zugriff auf die Datenbank von Kaspersky mit ständig aktualisierten Informationen über die Reputation von Dateien, Web-Ressourcen und Software gewährleistet. Kaspersky Security Network gewährleistet eine schnellere Reaktion der Programme von Kaspersky 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 Security Center Cloud Console

Ein Benutzerkonto, das Sie haben müssen, um Kaspersky Security Center Cloud Console 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 Security Center Cloud Console verwenden.

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 einen manuellen Start der Installation aus dem Programmpaket des Programms zur Gewährleistung der Sicherheit oder manuellen Start eines veröffentlichten Installationspakets, das zuvor auf das Gerät heruntergeladen wurde, voraussetzt.

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

Programmeinstellungen, die für alle Aufgabentypen gleich sind und den Gesamtbetrieb des Programms regeln, zum Beispiel Leistungseinstellungen, Berichtseinstellungen und Backup-Einstellungen.

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-Programmen mithilfe der von Kaspersky Security Center Cloud Console bereitgestellten Dienste.

Richtlinie

Eine Richtlinie bestimmt die Einstellungen eines Programms und verwaltet die Möglichkeit, dieses Programm auf Computern innerhalb einer Administrationsgruppe zu konfigurieren. Für jedes Programm 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, ein Programm von Kaspersky 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 eines Programms von Kaspersky 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 Programm-Module), 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

Satz von Updates für Programm-Module von Kaspersky 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 ihnen manuell Verteilungspunkte zu.

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 Security Center Cloud Console, 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 Security Center Cloud Console. Das Verwaltungs-Plug-in ist eine Schnittstelle zwischen Kaspersky Security Center Cloud Console und einem spezifischen Programm von Kaspersky. 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 Security Center Cloud Console bereitgestellt werden.

Zusätzlicher Abonnementschlüssel

Ein Schlüssel, der das Recht auf Nutzung des Programms bestätigt, jedoch im Augenblick nicht aktiviert ist.

Informationen über den Code von Drittherstellern

Informationen über den Code von Drittherstellern finden Sie in der Datei legal_notices.txt.

Die Datei "legal_notices.txt" befindet sich außerdem in den Installationsordnern des Administrationsagenten für Windows und des Administrationsagenten für Linux.

Weitere Informationen über den für Arbeitsbereiche verwendeten Code von Drittherstellern entnehmen Sie der Dokumentation von Kaspersky Endpoint Security Cloud.

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 Web Services und AWS sind Markenzeichen von Amazon.com, Inc. oder von verbundenen Unternehmen.

Apache und Apache feather logo sind Markenzeichen von The Apache Software Foundation.

Apple, App Store, AppleScript, FileVault, 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, XenServer sind Markenzeichen von Citrix Systems, Inc. und/oder einem oder mehreren seiner Tochtergesellschaften, und können im United States Patent and Trademark Office und in weiteren Ländern eingetragen sein.

Cloudflare, das Cloudflare-Logo und Cloudflare Workers sind Markenzeichen und/oder eingetragene Markenzeichen von Cloudflare, Inc. in den USA und anderen Gerichtsbarkeiten.

Corel ist ein Markenzeichen oder ein eingetragenes 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.

EulerOS ist ein Markenzeichen von Huawei Technologies Co., Ltd.

Intel und Core sind Markenzeichen der Intel Corporation in den USA und/oder anderen Ländern.

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 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.

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 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 und 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 Symbian-Markenzeichen ist Eigentum der Symbian Foundation Ltd.

VMware, VMware vSphere und VMware Workstation sind eingetragene Markenzeichen oder Markenzeichen von VMware, Inc. in den USA und/oder anderen Ländern.

UNIX ist ein in den USA und in anderen Ländern eingetragenes Markenzeichen, welches exklusiv durch die X/Open Company Limited lizenziert wird.