kaspersky

Kaspersky Security Center 14 Linux

Inhalt

Hilfe zu Kaspersky Security Center 14 Linux

	**Neuerungen** Erfahren Sie, was in der aktuellsten Version der Anwendung neu ist.		**Kaspersky-Programme. Lizenzverwaltung und Aktivierung** Aktivieren Sie die Programme von Kaspersky mit wenigen einfachen Schritten.
	**Hard- und Softwarevoraussetzungen** Überprüfen Sie, welche Betriebssysteme und Anwendungsversionen unterstützt werden.		**Netzwerkschutz konfigurieren** Verwalten Sie die Sicherheit der Organisation.
	**Installation** Administrationsserver und Kaspersky Security Center 14 Web Console installieren.		**Kaspersky-Programme. Datenbanken-Update und Update der Programm-Module** Sorgen Sie für die ununterbrochene Zuverlässigkeit des Schutzsystems.
	**Geräte im Netzwerk finden** Finden Sie vorhandene und neue Geräte im Netzwerk Ihres Unternehmens.		**Überwachung und Berichterstattung** Zeigen Sie Ihre Infrastruktur, den Schutzstatus und Statistiken an.
	**Kaspersky-Programme. Zentralisierte Softwareverteilung** Softwareverteilung für Programme von Kaspersky.		**Verteilungspunkte und/oder Verbindungs-Gateways anpassen** Konfigurieren Sie die Verteilungspunkte.

Neuerungen

Kaspersky Security Center 14 Linux

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

- Antiviren-Datenbanken für Kaspersky-Sicherheitsanwendungen können jetzt neben der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* auch durch die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* heruntergeladen werden.

- Die Antiviren-Datenbanken und Programm-Module auf den verwalteten Geräten können über einen Administrationsserver oder über Verteilungspunkte verbreitet und aktualisiert werden. Sie können ein optimales Update-Schema für Ihr Unternehmen auswählen, um die Belastung des Administrationsservers zu reduzieren und den Datenverkehr im Unternehmensnetzwerk zu optimieren.

- Kaspersky Security Center lädt von den Kaspersky-Update-Servern nur die Updates herunter, die von den Kaspersky-Sicherheits-Apps angefordert werden. Dadurch wird die Größe der heruntergeladenen Daten reduziert.

- Für den Download von Antiviren-Datenbanken und Programm-Modulen können Sie jetzt die Funktion für Diff-Dateien verwenden. Eine Diff-Datei beschreibt den Unterschied zwischen zwei Versionen der Datei einer Datenbank oder eines Programm-Moduls. Die Verwendung von Diff-Dateien entlastet den Datenverkehr in Ihrem Unternehmensnetzwerk, da Diff-Dateien weniger Platz einnehmen als die vollständigen Dateien der Datenbanken und Software-Module.

- Die Aufgabe *Update-Prüfung* wurde hinzugefügt. Mit dieser Aufgabe können Sie die heruntergeladenen Updates automatisch auf Funktionsfähigkeit und Fehler überprüfen, bevor Sie die Updates auf den verwalteten Geräten installieren.

Über Kaspersky Security Center Linux

In diesem Abschnitt werden die Konzeption, die Hauptfunktionen und die Komponenten von Kaspersky Security Center Linux erläutert.

Kaspersky Security Center Linux (auch Kaspersky Security Center genannt) 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.

Mit Kaspersky Security Center Linux können Sie Kaspersky-Sicherheits-Apps auf Geräten in einem Unternehmensnetzwerk installieren, Untersuchungs- und Update-Aufgaben per Fernzugriff ausführen und die Sicherheitsrichtlinien verwalteter Apps verwalten. Als Administrator verfügen Sie über ein umfassendes Dashboard, das einen Überblick über den Status der Unternehmensgeräte, ausführliche Berichte und Schutzrichtlinien mit detaillierten Einstellungen bereitstellt.

Kaspersky Security Center Linux hat einen anderen Funktionsumfang als Kaspersky Security Center mit einem Windows®-basierten Administrationsserver.

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

Kaspersky Security Center bietet Ihnen folgende Möglichkeiten:

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

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

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

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

- Apps von Kaspersky und anderen Softwareanbietern per Fernzugriff installieren.

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

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

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

- Inventarisierung der mit dem Unternehmensnetzwerk verbundenen Hardware durchführen.

- Dateien, die von den Sicherheitsanwendungen in die Quarantäne oder ins Backup verschoben wurden, sowie Dateien, deren Verarbeitung durch die Sicherheitsanwendungen aufgeschoben wurde, zentral verwalten.

Lieferumfang

Sie können das Programm über den Online-Shop von Kaspersky (beispielsweise auf https://www.kaspersky.de) oder über unsere Partnerunternehmen erwerben.

Beim Kauf von Kaspersky Security Center Linux in einem Online-Shop kopieren Sie das Programm von der Website des Online-Shops. Sie erhalten die zur Programmaktivierung erforderlichen Informationen nach Eingang des Rechnungsbetrags per E-Mail.

Hard- und Softwarevoraussetzungen

Administrationsserver

Hardwaremindestvoraussetzungen:

- CPU mit einer Taktfrequenz von 1 GHz oder höher. Für 64-Bit-Betriebssysteme beträgt die minimale Taktfrequenz des Prozessors 1.4 GHz.
- RAM: 4 GB.
- Freier Speicherplatz auf dem Datenträger: 10 GB.

Die folgenden Betriebssysteme werden unterstützt:

- 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 20.04 LTS (Focal Fossa) 64-Bit
- Ubuntu Server 18.04 LTS (Bionic Beaver) 64-Bit
- CentOS 7.x 64-Bit
- Red Hat Enterprise Linux Server 8.x 64-Bit
- Red Hat Enterprise Linux Server 7.x 64-Bit
- SUSE Linux Enterprise Server 12 (alle Service Packs) 64-Bit
- SUSE Linux Enterprise Server 15 (alle Service Packs) 64-Bit
- Astra Linux Special Edition 1.7 (einschließlich Modus für abgeschlossene Softwareumgebungen und obligatorischem Modus) 64-Bit
- Astra Linux Special Edition 1.6 (einschließlich des Modus für abgeschlossene Softwareumgebungen und des obligatorischen Modus) 64-Bit
- Astra Linux Common Edition 2.12 64-Bit
- Alt Server 10 64-Bit
- Alt Server 9.2 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
- Oracle Linux 7 64-Bit
- Oracle Linux 8 64-Bit
- RED OS 7.3 Server 64-Bit
- RED OS 7.3 Certified Edition 64-Bit

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
- Parallels Desktop 17
- Kernel-basierte virtuelle Maschine. Unterstützt die folgenden Betriebssysteme:
  - Alt 8 SP Server (LKNV.11100-01) 64-Bit
  - Alt Server 10 64-Bit
  - Astra Linux Special Edition 1.7 (einschließlich Modus für abgeschlossene Softwareumgebungen und obligatorischem Modus) 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 Server 64-Bit
  - RED OS 7.3 Certified Edition 64-Bit

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

- MySQL 5.7 Community 32-Bit/64-Bit

- MySQL 8.0 32-Bit/64-Bit
- MariaDB 10.5.x 32-Bit/64-Bit
- MariaDB 10.4.x 32-Bit/64-Bit
- MariaDB 10.3.22 und höher 32-Bit/64-Bit
- MariaDB Server 10.3 32-Bit/64-Bit mit InnoDB Storage Engine
- MariaDB 10.1.30 und höher 32-Bit/64-Bit

Kaspersky Security Center 14 Web Console

Kaspersky Security Center 14 Web Console Server

Hardwaremindestvoraussetzungen:

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

Eines der folgenden Betriebssysteme (nur 64-Bit-Versionen):

- Debian GNU/Linux 11.x (Bullseye)
- Debian GNU/Linux 10.x (Buster)
- Debian GNU/Linux 9.x (Stretch)
- Ubuntu Server 20.04 LTS (Focal Fossa)
- Ubuntu Server 18.04 LTS (Bionic Beaver)
- CentOS 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 7.x
- SUSE Linux Enterprise Server 12 (alle Service Packs)
- SUSE Linux Enterprise Server 15 (alle Service Packs)
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64-Bit
- Astra Linux Special Edition 1.7 (einschließlich Modus für abgeschlossene Softwareumgebungen und obligatorischem Modus)
- Astra Linux Special Edition 1.6 (einschließlich des Modus für abgeschlossene Softwareumgebungen und des obligatorischen Modus)

- Astra Linux Common Edition 2.12
- Alt Server 10
- Alt Server 9.2
- Alt 8 SP Server (LKNV.11100-01)
- Alt 8 SP Server (LKNV.11100-02)
- Alt 8 SP Server (LKNV.11100-03)
- Oracle Linux 8
- Oracle Linux 7
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition

Unter den Virtualisierungsplattformen werden Kernel-basierte virtuelle Maschinen für folgende Betriebssysteme unterstützt:

- Alt 8 SP Server (LKNV.11100-01) 64-Bit
- Alt Server 10 64-Bit
- Astra Linux Special Edition 1.7 (einschließlich Modus für abgeschlossene Softwareumgebungen und obligatorischem Modus) 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 Server 64-Bit
- RED OS 7.3 Certified Edition 64-Bit

Client-Geräte

Für die Nutzung von Kaspersky Security Center 14 Web Console auf einem Client-Gerät ist nur ein Browser erforderlich.

Die Hard- und Softwarevoraussetzungen für das Gerät entsprechen den Anforderungen des Browsers, der für die Arbeit mit Kaspersky Security Center 14 Web Console verwendet wird.

Browser:

- Mozilla Firefox Extended Support Release 91.8.0 oder höher (91.8.0 veröffentlicht am 5. April 2022)
- Mozilla Firefox Release 99.0 oder höher (99.0 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.

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

Die folgenden Betriebssysteme werden unterstützt:

- 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 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 8.x 64-Bit
- CentOS 7.x 64-Bit
- CentOS 7.x ARM 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 1.7 (einschließlich Modus für abgeschlossene Softwareumgebungen und obligatorischem Modus) 64-Bit
- Astra Linux Special Edition 1.6 (einschließlich des Modus für abgeschlossene Softwareumgebungen und des obligatorischen Modus) 64-Bit
- Astra Linux Common Edition 2.12 64-Bit
- Astra Linux Special Edition 4.7 ARM
- 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
- Mageia 4 32-Bit
- Oracle Linux 7 64-Bit
- Oracle Linux 8 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 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
- Lotos (Linux Core-Version 4.19.50, DE: MATE) 64-Bit

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:
  - Alt 8 SP Server (LKNV.11100-01) 64-Bit
  - Alt Server 10 64-Bit
  - Astra Linux Special Edition 1.7 (einschließlich Modus für abgeschlossene Softwareumgebungen und obligatorischem Modus) 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

Es wird empfohlen, den Administrationsagenten für Linux mit gleichen Version wie zu installieren, wie Kaspersky Security Center Linux.

Über die Kaspersky Security Center 14 Web Console

Kaspersky Security Center 14 Web Console ist ein Programm (eine Web-App), welches dafür konzipiert ist, den Sicherheitsstatus der Unternehmensnetzwerke zu kontrollieren, die mit Kaspersky-Programmen geschützt werden.

Mithilfe des Programms können Sie folgende Aktionen ausführen:

- Status des Antiviren-Schutzsystems in Ihrem Unternehmen kontrollieren.
- Programme von Kaspersky auf Geräten Ihres Netzwerks installieren und die installierten Programme verwalten.
- Für die Geräte Ihres Netzwerks erstelle Richtlinien verwalten.
- Benutzerkonten verwalten.
- Aufgaben für Programme verwalten, die auf Ihren Netzwerkgeräten installiert sind.
- Berichte über den Schutzstatus anzeigen.
- Versand von Berichten an Systemadministratoren und andere IT-Spezialisten verwalten.

Das Programm Kaspersky Security Center 14 Web Console stellt eine Weboberfläche zur Verfügung, die Ihre Interaktion mit dem Administrationsserver durch den Browser gewährleistet. Beim Administrationsserver handelt es sich um ein Programm, das für die Verwaltung der auf Ihren Netzwerkgeräten installierten Kaspersky-Programme konzipiert ist. Der Administrationsserver verbindet sich mit den Geräten Ihres Netzwerks über die geschützten (SSL) Kommunikationskanäle. Wenn Sie mithilfe Ihres Browsers eine Verbindung zur Kaspersky Security Center 14 Web Console herstellen, stellt der Browser eine sichere Verbindung mit dem Server von Kaspersky Security Center 14 Web Console her.

Kaspersky Security Center 14 Web Console funktioniert auf folgende Weise:

1. Sie stellen eine Verbindung zur Kaspersky Security Center 14 Web Console mithilfe Ihres Browsers her, in dessen Fenster die Seiten des Programm-Webportals angezeigt werden.
2. Mithilfe der Verwaltungselemente des Webportals wählen Sie einen Befehl, den Sie ausführen möchten. Kaspersky Security Center 14 Web Console führt folgende Aktionen aus:
    - Wenn Sie einen Befehl zum Empfangen von Informationen ausgewählt haben (z. B. Geräteliste anzeigen), erstellt Kaspersky Security Center 14 Web Console eine entsprechende Abfrage an den Administrationsserver, empfängt danach die erforderlichen Daten vom Server und leitet sie in einer zur Anzeige geeigneten Ansicht an den Browser weiter.
    - Wenn Sie einen Verwaltungsbefehl ausgewählt haben (z.B. Remote-Installation eines Antiviren-Programms), empfängt Kaspersky Security Center 14 Web Console den Befehl vom Browser und leitet ihn an den Administrationsserver weiter. Danach empfängt das Programm vom Administrationsserver das Ergebnis der Befehlsausführung und leitet es in einer zur Anzeige geeigneten Ansicht an den Browser weiter.

Kaspersky Security Center 14 Web Console ist eine mehrsprachige Anwendung. Sie können die Sprache der Benutzeroberfläche jederzeit und ohne erneutes Öffnen der Anwendung ändern. Wenn Sie Kaspersky Security Center 14 Web Console zusammen mit Kaspersky Security Center installieren, besitzt Kaspersky Security Center 14 Web Console die gleiche Sprache für die Benutzeroberfläche, wie die Installationsdatei. Wenn Sie Kaspersky Security Center 14 Web Console separat installieren, besitzt die Anwendung die gleiche Sprache für die Benutzeroberfläche, wie das Betriebssystem. Wenn Kaspersky Security Center 14 Web Console die Sprache der Installationsdatei oder des Betriebssystems nicht unterstützt, wird standardmäßig Englisch festgelegt.

Liste der unterstützten Programme von Kaspersky

Kaspersky Security Center Linux unterstützt die zentralisierte Bereitstellung und Verwaltung von Kaspersky Endpoint Security für Linux. Dieses Programm ermöglicht den Schutz von Arbeitsstationen und Dateiservern. Informationen über die Programmversionen finden Sie auf der Webseite zum Lebenszyklus des Produkt-Supports.

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

Kaspersky bietet Kaspersky Security Center als lokale Lösung für zwei Plattformen – Windows und Linux. Bei der Windows-basierten Lösung installieren Sie den Administrationsserver auf einem Windows-Gerät und bei der Linux-basierten Lösung ist die Administrationsserver-Version für die Installation auf einem Linux-Gerät vorgesehen.

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

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

Funktion oder Eigenschaft	Kaspersky Security Center	
	Windows-basierte Lösung	**Linux-basierte Lösung**
Standort des Administrationsservers	On-premises	On-premises
Standort des Datenbankmanagementsystems (DBMS)	On-premises	On-premises
Betriebssystem, auf dem der Administrationsserver installiert werden soll	Windows	Linux
Typ der Verwaltungskonsole	Lokal und webbasiert	Webbasiert
Betriebssystem, auf dem die webbasierte Verwaltungskonsole installiert werden soll	Windows oder Linux	Windows oder Linux
Hierarchie des Administrationsservers	✓	✓
Hierarchie der Administrationsgruppen	✓	✓
Netzwerkabfrage	✓	✓ (nur nach IP-Bereichen)
Maximale Anzahl verwalteter Geräte	100000	20000
Schutz von verwalteten Windows-, macOS- und Linux-verwalteten Geräten	✓	– (Schutz nur von Linux-Geräten)
Schutz von mobilen Geräten	✓	–
Schutz von virtuellen Maschinen	✓	–
Schutz der Public-Cloud-Infrastruktur	✓	–

Gerätezentriertes Sicherheitsmanagement	✓	✓
Benutzerzentriertes Sicherheitsmanagement	✓	✓
Programmrichtlinien	✓	✓
Aufgaben für Kaspersky-Programme	✓	✓
Kaspersky Security Network	✓	–
KSN-Proxy	✓	–
Kaspersky Private Security Network	✓	–
Zentralisierte Bereitstellung von Lizenzschlüsseln für Kaspersky-Programme	✓	✓
Unterstützung für virtuelle Administrationsserver	✓	✓
Installieren von Software-Updates von Drittanbietern und Beheben von Schwachstellen in Programmen von Drittanbietern	✓	– (nur für Verwendung einer Remote-Installationsaufgabe)
Benachrichtigungen über Ereignisse, die auf verwalteten Geräten auftreten	✓	✓
Erstellen und Verwalten von Benutzerkonten	✓	✓
Statusüberwachung für Richtlinien und Aufgaben	✓	✓
Bereitstellung des Kaspersky-Failover-Clusters	✓	✓

Grundbegriffe

In diesem Abschnitt werden die Grundbegriffe von Kaspersky Security Center Linux erläutert.

Administrationsserver

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

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

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

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

Der Administrationsserver führt folgende Funktionen aus:

- Speicherung der Struktur der Administrationsgruppen
- Speicherung von Informationen über die Konfiguration der Client-Geräte
- Organisation der Datenverwaltung für Programmpakete
- Remote-Installation von Programmen auf Client-Geräten und Löschen von Programmen
- Datenbanken-Update und Update der Programm-Module von Kaspersky
- Verwaltung von Richtlinien und Aufgaben auf Client-Geräten
- Speicherung von Informationen über die auf den Client-Geräten aufgetretenen Ereignisse
- Erstellen von Berichten über die Ausführung von Kaspersky-Programmen
- Verteilung von Lizenzschlüsseln auf Client-Geräte, sowie Speicherung von Informationen über die Lizenzschlüssel
- Senden von Benachrichtigungen über den Status der Aufgabenausführung (z. B. über einen Virenfund auf einem Client-Gerät)

Namensgebung für Administrationsserver in der Programmoberfläche

Auf der Benutzeroberfläche von Kaspersky Security Center 14 Web Console können Administrationsserver die folgenden Namen haben:

- Name des Geräts mit dem Administrationsserver, z. B. "*Gerätename*" oder "Administrationsserver: *Gerätename*".

- IP-Adresse des Geräts mir dem Administrationsserver, z. B. "*IP-Adresse*" oder "Administrationsserver: *IP-Adresse*".

- Sekundäre Administrationsserver und virtuelle Administrationsserver haben benutzerdefinierte Namen, die Sie beim Verbinden eines virtuellen oder sekundären Administrationsservers mit dem primären Administrationsserver angeben.

- Wenn Sie Kaspersky Security Center 14 Web Console auf einem Linux-Gerät installiert haben und verwenden, zeigt das Programm die Namen von Administrationsservern, die Sie als "vertrauenswürdig" eingestuft haben, in einer Antwort-Datei an.

Sie können über Kaspersky Security Center 14 Web Console eine Verbindung zum Administrationsserver herstellen.

Hierarchie des Administrationsservers

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

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

In einer Hierarchie kann der Linux-Administrationsserver von Kaspersky Security Center nur als sekundärer Server fungieren, der von einem primären Administrationsserver des Windows-basierten Kaspersky Security Center oder Kaspersky Security Center Cloud Console verwaltet wird.

Die Hierarchie der Administrationsserver lässt sich zu folgenden Zwecken verwenden:

- Beschränkung der Belastung des Administrationsservers (im Vergleich zu einem einzigen im Netzwerk installierten Server).

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

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

- Nutzung von Kaspersky Security Center von Dienstanbietern. Ein Dienstanbieter muss lediglich Kaspersky Security Center und die Kaspersky Security Center 14 Web Console installieren. Um eine große Anzahl an Client-Geräten verschiedener Unternehmen zu verwalten, kann der Dienstanbieter virtuelle Administrationsserver zur Hierarchie der Administrationsserver hinzufügen.

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

Virtueller Administrationsserver

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

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

- Ein virtueller Administrationsserver kann nur auf einem primären Administrationsserver erstellt werden.
- Ein virtueller Administrationsserver verwendet während seines Betriebs die Datenbank des primären Administrationsservers. Aufgaben zum Backup und zur Wiederherstellung von Dateien, sowie Aufgaben zur Suche nach Updates und Downloadaufgaben werden von einem virtuellen Administrationsserver nicht unterstützt.
- Für virtuelle Server können keine sekundären Administrationsserver angelegt werden (einschließlich virtueller Server).

Außerdem weisen virtuelle Administrationsserver folgende Einschränkungen auf:

- Im Eigenschaftenfenster des virtuellen Administrationsservers ist die Anzahl der Abschnitte beschränkt.
- Um eine Remote-Installation von Kaspersky-Programmen auf Client-Geräten vorzunehmen, die vom virtuellen Administrationsserver verwaltet werden, muss auf einem der Computer der Administrationsagent installiert sein, über den eine Verbindung zum virtuellen Administrationsserver aufgebaut werden kann. Beim ersten Verbindungsaufbau zum virtuellen Administrationsserver wird diesem Computer automatisch die Rolle des Verteilungspunkts zugewiesen, sodass er als Verbindungs-Gateway für den Anschluss von Client-Geräten an den virtuellen Administrationsserver dient.
- Der virtuelle Server kann das Netzwerk nur über die Verteilungspunkte durchsuchen.
- Um einen nicht voll funktionsfähigen virtuellen Server neu zu starten, startet Kaspersky Security Center Linux den primären Administrationsserver und alle virtuellen Administrationsserver neu.

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

Webserver

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

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

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

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

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

```
https://<Webservername>:<HTTPS-Port>/public/<Objekt>
```

wobei:

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

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

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

Administrationsagent

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

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

- Unter dem Namen "Kaspersky Security Center 14 Linux Administrationsagent"
- Mit automatischem Start bei Start des Betriebssystems
- Unter Verwendung des Kontos "LocalSystem"

Ein Gerät, auf dem der Administrationsagent installiert ist, wird als *verwaltetes Gerät* oder *Gerät* bezeichnet. Den Administrationsagenten können Sie aus einer der folgenden Quellen installieren:

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

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

Die Namen des Prozesses, den der Administrationsagent startet, lauten wir folgt:

- klnagent64.service (für 64-Bit-Betriebssysteme)
- klnagent.service (für 32-Bit-Betriebssysteme)

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

Administrationsgruppen

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

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

- Verwenden derselben 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.

Verwaltetes Gerät

Ein *verwaltetes Gerät* ist ein Computer, der unter Linux läuft und auf dem der Administrationsagent installiert ist. Sie können solche Geräte verwalten, indem Sie Aufgaben und Richtlinien für auf diesen Geräten installierte Anwendungen erstellen. Sie können auch Berichte von verwalteten Geräten beziehen.

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

Ein Gerät kann nur von einem Administrationsserver verwaltet werden. Ein Administrationsserver kann bis zu 20.000 Geräte verwalten.

Nicht zugeordnetes Gerät

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

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

Administrator-Arbeitsplatz

Geräte, auf denen der Server der Kaspersky Security Center 14 Web Console installiert ist, werden als *Administrator-Arbeitsplätze* bezeichnet. Von diesen Geräten aus können die Administratoren eine zentralisierte Remote-Programmverwaltung für die auf den Client-Geräten installierten Kaspersky-Programme durchführen.

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

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

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

Web-Plug-ins zur Verwaltung

Für die Remote-Verwaltung der Software von Kaspersky mithilfe von Kaspersky Security Center 14 Web Console wird eine spezielle Komponente – das *Web-Plug-in zur Verwaltung* – verwendet. Im Weiteren wird das Web-Plug-in zur Verwaltung als *Verwaltungs-Plug-in* bezeichnet. Das Verwaltungs-Plug-in ist eine Schnittstelle zwischen Kaspersky Security Center 14 Web Console und einem spezifischen Programm von Kaspersky. Mit einem Verwaltungs-Plug-in können Sie Aufgaben und Richtlinien für die Anwendung konfigurieren.

Sie können die Web-Plug-ins zur Verwaltung von der Webseite des Kundendienstes von Kaspersky herunterladen.

Das Verwaltungs-Plug-in stellt Folgendes bereit:

- Schnittstelle zum Erstellen und Ändern von Aufgaben und Einstellungen für Anwendungen
- Schnittstelle zum Erstellen und Ändern von Richtlinien und Richtlinienprofilen für die ferngesteuerte und zentralisierte Konfiguration von Kaspersky-Programmen und Geräten
- Übertragung von Ereignissen, die von der Anwendung erzeugt wurden
- Kaspersky Security Center 14 Web Console funktioniert für die Anzeige von Betriebsdaten und Ereignissen der Anwendung sowie von Statistiken, die von Client-Geräten weitergeleitet wurden

Richtlinien

Eine *Richtlinie* besteht aus einer Reihe von 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 bietet eine einzelne Richtlinie für jedes Kaspersky-Programm in einer Administrationsgruppe. Eine Richtlinie hat eine der folgenden Statusvarianten:

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.
- 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 erfüllt ist.
- Richtlinienprofile enthalten Werte für Einstellungen, die von den Richtlinieneinstellungen abweichen.
- Durch das Aktivieren eines Richtlinienprofils werden die effektiven Einstellungen des verwalteten Gerätes geändert.
- Eine Richtlinie kann nicht mehr als 100 Richtlinienprofile enthalten.

Richtlinienprofile

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

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

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

Aufgaben

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

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

Aufgaben können auf dem Administrationsserver und auf Geräten ausgeführt werden.

Die folgenden Aufgaben werden auf dem Administrationsserver ausgeführt:

- Berichte automatisch versenden
- Updates in die Datenverwaltung des Administrationsservers herunterladen
- Backup der Daten des Administrationsservers anlegen
- Datenbank bedienen
- Installationspaket anhand des Betriebssystem-Abbilds eines Mustergeräts erstellen

Die folgenden Typen von Aufgaben werden auf Geräten ausgeführt:

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

  Lokale Aufgaben können nicht nur vom Administrator mithilfe von Kaspersky Security Center 14 Web Console geändert werden, sondern auch vom Benutzer des Remote-Gerätes (beispielsweise in der Benutzeroberfläche der Sicherheits-App). Wenn eine lokale Aufgabe gleichzeitig sowohl vom Administrator als auch vom Benutzer auf dem verwalteten Gerät geändert wurde, treten jene Änderungen in Kraft, die vom Administrator mit höherer Priorität ausgeführt wurden.

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

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

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

Sie können für jedes Programm eine beliebige Anzahl von Gruppenaufgaben, globalen Aufgaben oder lokalen Aufgaben erstellen.

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

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

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

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

Aufgabenumfang

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

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

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

- Bestimmte Geräte manuell festlegen.

  Als Adresse des Gerätes können Sie eine IP-Adresse (oder einen IP-Bereich) oder einen 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.

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.

Den Wert, den das Programm auf dem Client-Gerät verwendet (s. Abb. unten), wird durch das Schloss (🔒) an der Einstellung in der Richtlinie 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.

Richtlinie und lokale Programmeinstellungen

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 unterbunden wurde.

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

Verteilungspunkt

Der *Verteilungspunkt* (bisher "Update-Agent") ist ein Gerät mit installiertem Administrationsagenten, das verwendet wird für die Update-Verteilung, die Remote-Installation von Programmen und den Empfang von Informationen über Geräte im Netzwerk. Der Verteilungspunkt kann folgende Funktionen ausführen:

- Updates und Installationspakete, die vom Administrationsserver heruntergeladen wurden, auf die Client-Geräte der Gruppe verteilen (einschließlich Verteilung durch Multicasting über das UDP-Protokoll). Updates können sowohl vom Administrationsserver als auch von den Kaspersky-Update-Servern empfangen werden. Im letzteren Fall muss für den Verteilungspunkt eine Update-Aufgabe erstellt werden.

  Verteilungspunkte beschleunigen die Update-Verteilung und ermöglichen, die Belastung des Administrationsservers zu verringern.

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

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

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

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

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

- Remote-Installation von Kaspersky-Programmen und von Programmen anderer Softwareanbietern, einschließlich der Installation auf Client-Geräten ohne Administrationsagent.

  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.

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

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

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

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

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

Administrationsagenten mit einem aktiven Verbindungsprofil nehmen nicht an der Ermittlung der Broadcast-Domäne teil.

Kaspersky Security Center Linux weist jedem Administrationsagenten eine eindeutige Adresse für den 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. Adressen für IP-Versand an mehrere Adressen, die schon in den vorigen Programmversionen zugewiesen wurden, werden nicht geändert.

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 klnagchk-Bericht 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 Laufwerk 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.

Verbindungs-Gateway

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

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

Sie haben zwei Möglichkeiten, Verbindungs-Gateways zu verwenden:

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

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

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

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

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

Lizenzierung

Dieser Abschnitt informiert über die grundlegenden Konzepte, die mit der Lizenzierung von Kaspersky Security Center 14 Linux zusammenhängen.

Über den Endbenutzer-Lizenzvertrag

Der *Endbenutzer-Lizenzvertrag* (Lizenzvertrag oder EULA) ist ein rechtsgültiger Vertrag zwischen Ihnen und AO Kaspersky Lab. Er bestimmt die Nutzungsbedingungen für das Programm.

Bitte lesen Sie sich den Endbenutzer-Lizenzvertrag sorgfältig durch, bevor Sie das Programm nutzen.

Kaspersky Security Center Linux und die einzelnen Komponenten (z. B. Administrationsagent) haben jeweils eine eigene EULA.

Sie können die Bedingungen des Endbenutzer-Lizenzvertrags für Kaspersky Security Center Linux wie folgt anzeigen:

- Während der Installation von Kaspersky Security Center.
- Mithilfe des Dokuments license.txt, das zum Lieferumfang von Kaspersky Security Center gehört.
- Mithilfe des Dokuments license.txt im Installationsordner von Kaspersky Security Center.

Sie können die Bedingungen des Endbenutzer-Lizenzvertrags für den Administrationsagenten für Linux wie folgt anzeigen:

- Während das Distributionspaket für den Administrationsagenten von den Kaspersky-Webservern heruntergeladen wird.
- Während der Installation des Administrationsagenten für Linux.

  Bitte beachten Sie, dass bei der Installation des Administrationsagenten für Linux der Endbenutzer-Lizenzvertrag für den Administrationsagenten in englischer Sprache angezeigt wird. Sie können den Endbenutzer-Lizenzvertrag für den Administrationsagenten in anderen Sprachen im Ordner /opt/kaspersky/klnagent64/share/license einsehen, bevor Sie die Bedingungen des Endbenutzer-Lizenzvertrags während der Installation akzeptieren.

- Im Dokument license.txt, das im Distributionspaket des Administrationsagenten für Linux enthalten ist.
- Im Dokument license.txt, das sich im Installationsordner des Administrationsagenten für Linux befindet.

Wenn Sie bei der Programminstallation dem Text des Endbenutzer-Lizenzvertrags zustimmen, gelten die Bedingungen des Endbenutzer-Lizenzvertrags als akzeptiert. Falls Sie den Lizenzvertrag ablehnen, brechen Sie die Programminstallation ab und nutzen Sie das Programm nicht.

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 Linux 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.

  Nachdem die Gültigkeit der kommerziellen Lizenz abgelaufen ist, setzt das Programm seine Arbeit mit eingeschränkter Funktionalität fort (z. B. sind keine Datenbanken-Updates für Kaspersky Security Center möglich). Zur weiteren Nutzung von Kaspersky Security Center ist eine Verlängerung der kommerziellen Lizenz erforderlich.

Es wird empfohlen, die Gültigkeitsdauer der Lizenz vor dem Ablaufdatum zu verlängern, um einen optimalen Schutz vor allen Bedrohungen der Sicherheit 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 einen Lizenzschlüssel mithilfe einer der folgenden Methoden zur Anwendung hinzufügen: durch Anwendung einer *Schlüsseldatei* oder Eingabe eines *Aktivierungscodes*. 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.

Anzeigen der Datenschutzrichtlinie

Die Datenschutzrichtlinie ist online verfügbar unter https://www.kaspersky.de/products-and-services-privacy-policy.

Die Datenschutzrichtlinie ist auch offline verfügbar:

- Sie können die Datenschutzrichtlinie lesen, bevor Sie Kaspersky Security Center installieren.
- Der Text der Datenschutzrichtlinie ist in der Datei license.txt im Installationsordner von Kaspersky Security Center enthalten.
- Die Datei privacy_policy.txt ist auf einem verwalteten Gerät im Installationsordner des Administrationsagenten verfügbar.
- Sie können die Datei privacy_policy.txt aus dem Distributionspaket des Administrationsagenten entpacken.

Varianten der Lizenzierung von Kaspersky Security Center

Kaspersky Security Center wird als Teil der Kaspersky-Programme zum Schutz von Unternehmensnetzwerken bereitgestellt. Außerdem steht es auf der Website von Kaspersky zum Download bereit.

Es stehen folgende Funktionen zur Verfügung:

- Virtuelle Administrationsserver erstellen, um ein Netzwerk entfernter Standorte bzw. Kundenunternehmen zu verwalten
- Hierarchie der Administrationsgruppen erstellen, um eine Reihe von Geräten als Ganzes zu verwalten
- Status der Antiviren-Sicherheit eines Unternehmens kontrollieren
- Remote-Installation von Programmen
- Liste der Betriebssystem-Abbilder anzeigen, die für die Remote-Installation verfügbar sind
- Einstellungen der auf den Client-Geräten installierten Programme zentral anpassen
- Vorhandene lizenzierte Programmgruppen anzeigen und ändern
- Statistiken und Berichte über die Ausführung von Programmen sowie Benachrichtigungen über kritische Ereignisse erhalten
- Liste der durch eine Netzwerkabfrage gefundenen Geräte anzeigen und manuell bearbeiten
- Zentral Dateien verwalten, die in die Quarantäne, ins Backup oder in die Ablage für Dateien mit verschobener Verarbeitung verschoben wurden
- Benutzerrollen verwalten

Über die Schlüsseldatei

Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung key, die Sie von Kaspersky erhalten. Schlüsseldateien dienen zum Aktivieren der Anwendung durch Hinzufügen eines Lizenzschlüssels.

Sie erhalten eine Schlüsseldatei an die E-Mail-Adresse, die Sie beim Kauf von Kaspersky Security Center oder bei der Anforderung der Testversion von Kaspersky Security Center angegeben haben.

Um das Programm mithilfe der Schlüsseldatei zu aktivieren, ist keine Verbindung mit den Kaspersky-Aktivierungsservern erforderlich.

Wenn die Schlüsseldatei versehentlich gelöscht wurde, können Sie sie wiederherstellen. Eine Schlüsseldatei kann beispielsweise für die Registrierung eines Kaspersky CompanyAccount erforderlich sein.

Um Ihre Schlüsseldatei wiederherzustellen, führen Sie eine der folgenden Aktionen aus:

- Wenden Sie sich an den Lizenzverkäufer.
- Schlüsseldatei anhand eines vorhandenen Aktivierungscodes auf der Website von Kaspersky abrufen.

Über die Bereitstellung von Daten

An den Rechteinhaber übermittelte Daten

Werden im Endbenutzer-Lizenzvertrag für Kaspersky Security Center 14 Linux aufgezählt.

Lokal verarbeitete Daten

Kaspersky Security Center Linux dient dazu, die wichtigsten Aufgaben zur Verwaltung und Wartung des Antiviren-Schutzes in einem Unternehmensnetzwerk zentral zu erledigen. Kaspersky Security Center Linux ermöglicht es einem Administrator, auf detaillierte Informationen über die Sicherheitsstufe des Unternehmensnetzwerks zuzugreifen. Mit Kaspersky Security Center Linux kann ein Administrator alle Schutzkomponenten konfigurieren, die auf Kaspersky-Programmen basieren. Die folgenden Hauptfunktionen werden von Kaspersky Security Center Linux ausgeführt:

- Erkennen von Geräten und deren Benutzern im Unternehmensnetzwerk
- Erstellen einer Hierarchie von Administrierungsgruppen für die Geräteverwaltung
- Installieren von Kaspersky-Programmen auf Geräten
- Verwalten der Einstellungen und Aufgaben von installierten Programmen
- Aktivieren von Kaspersky-Programmen auf Geräten
- Benutzerkonten verwalten
- Anzeigen von Informationen zum Betrieb von Kaspersky-Programmen auf Geräten
- Anzeigen von Berichten

Um seine Hauptfunktionen auszuführen, kann Kaspersky Security Center Linux die folgenden Informationen empfangen, speichern und verarbeiten:

- Informationen über die Geräte im Unternehmensnetzwerk, die infolge der Gerätesuche im Windows-Netzwerk oder über den Scan von IP-Intervallen erhalten wurden. Der Administrationsserver ruft seinerseits Daten ab oder empfängt Daten vom Administrationsagenten.
- 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 Gerätes auf der Benutzeroberfläche von Kaspersky Security Center 14 Web Console ein:
    - Technische Spezifikationen des verwalteten Geräts und seiner Komponenten, die zur Geräteidentifizierung erforderlich sind: Anzeigename und Beschreibung des Gerätes, DNS-Domäne und DNS-Name, IPv4-Adresse, IPv6-Adresse, Netzwerkadresse, MAC-Adresse, Betriebssystemtyp, ob das Gerät eine virtuelle Maschine mit Hypervisor-Typ ist oder ob das Gerät eine dynamische virtuelle Maschine als Teil von VDI ist.
    - Andere Spezifikationen der verwalteten Geräte und ihrer Komponenten, die für die Überprüfung verwalteter Geräte erforderlich sind: Betriebssystemarchitektur, Betriebssystemhersteller, Build-Nummer des Betriebssystems, Release-ID des Betriebssystems, Ordner des Speicherorts des Betriebssystems, wenn es sich bei dem Gerät um eine virtuelle Maschine handelt – der Typ der virtuellen Maschine.
    - Details zu Aktionen auf verwalteten Geräten: Datum und Uhrzeit des letzten Updates; Uhrzeit, zu der das Gerät zuletzt im Netzwerk sichtbar war; Neustart-Wartestatus; Uhrzeit, zu der das Gerät eingeschaltet wurde.
    - Details zu Gerätebenutzerkonten und den deren Arbeitssitzungen.
- Statistiken zum Verteilungspunkt-Betrieb, wenn das Gerät ein Verteilungspunkt ist. Der Administrationsagent übermittelt Daten von dem Gerät an den Administrationsserver.

- Vom Benutzer in Kaspersky Security Center 14 Web Console eingegebene Einstellungen für die Verteilungspunkte.

- Einzelheiten zu den auf dem Gerät installierten Anwendungen von Kaspersky. Die verwaltete Anwendung überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver:

  - Einstellungen der auf dem verwalteten Gerät installierten Kaspersky-Programme: Name und Version des Kaspersky-Programms, Status, Echtzeitschutzstatus, Datum und Uhrzeit der letzten Untersuchung des Geräts, Anzahl der erkannten Bedrohungen, Anzahl der Objekte, deren Desinfektion fehlgeschlagen ist, Verfügbarkeit und Status der Programmkomponenten, Details zu den Einstellungen und Aufgaben von Kaspersky-Programmen, Informationen zu aktiven und Reserve-Lizenzschlüsseln, Installationsdatum der Anwendung und ID.

  - Statistiken zur Anwendungsoperation: Ereignisse im Zusammenhang mit Statusveränderungen von Komponenten der Kaspersky-Programme auf dem verwalteten Gerät und im Zusammenhang mit der Ausführung von Aufgaben, die von den Softwarekomponenten ausgelöst werden.

  - Der Status des Geräts wird von dem Kaspersky-Programm bestimmt.

  - Von dem Kaspersky-Programm zugewiesene Tags.

- Daten, die in Ereignissen der Komponenten von Kaspersky Security Center Linux und der durch Kaspersky verwalteten Programmen enthalten sind. Der Administrationsagent übermittelt Daten von dem Gerät an den Administrationsserver.

- Einstellungen der Komponenten von Kaspersky Security Center Linux und der durch Kaspersky verwalteten Programme in Richtlinien und Richtlinienprofilen. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center 14 Web Console ein.

- Aufgabeneinstellungen der Komponenten von Kaspersky Security Center Linux und der durch Kaspersky verwalteten Programme. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center 14 Web Console ein.

- Von der Schwachstellen- und Patch-Management-Funktion verarbeitete Daten. Der Administrationsagent überträgt vom Gerät an den Administrationsserver Informationen über die auf den verwalteten Geräten erkannte Hardware (Hardware-Inventur).

- Benutzerkategorien der Anwendungen. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center 14 Web Console ein.

- Informationen über ausführbaren Dateien, die auf verwalteten Geräten durch die Komponente "Programmkontrolle" gefunden werden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.

- Details zu Dateien, die ins Backup verschoben wurden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.

- Details zu Dateien, die in die Quarantäne verschoben wurden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.

- Informationen zu Dateien, die von Kaspersky-Spezialisten für eine detaillierte Analyse angefordert wurden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.

- Informationen über externe Geräte (Speichereinheiten, Tools zum Informationstransfer, Hardcopy-Tools und Verbindungsbusse), die auf dem verwalteten Gerät installiert oder damit verbunden sind und von der Gerätekontrolle erkannt werden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.

- Liste der verwalteten speicherprogrammierbaren Steuerungen (SPS). Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.

- Einzelheiten zu den eingegebenen Aktivierungscodes. Der Benutzer gibt Daten in die Verwaltungskonsole oder in die Benutzeroberfläche von Kaspersky Security Center 14 Web Console ein.

- Benutzerkonten: Name, Beschreibung, vollständiger Name, E-Mail-Adresse, Haupttelefonnummer und Kennwort. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center 14 Web Console ein.

- Revisionsverlauf von verwalteten Objekten. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center 14 Web Console ein.

- Register der gelöschten Managementobjekte. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center 14 Web Console ein.

- Aus der Datei erzeugte Installationspakete wie auch Installationseinstellungen. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center 14 Web Console ein.

- Daten, die für die Anzeige für Neuigkeiten von Kaspersky in der Kaspersky Security Center 14 Web Console erforderlich sind. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center 14 Web Console ein.

- Daten, die für das Funktionieren von Plug-Ins verwalteter Anwendungen in Kaspersky Security Center 14 Web Console erforderlich sind und die von den Plug-Ins in der Datenbank des Administrationsservers während ihres Regelbetriebs gespeichert werden. Die Beschreibung und Möglichkeiten zur Bereitstellung der Daten finden Sie in den Hilfedateien der entsprechenden Anwendung.

- Benutzereinstellungen für Kaspersky Security Center 14 Web Console: Sprache und Schema der Benutzeroberfläche, Einstellungen für die Anzeige des Überwachungsfensters, Status der Benachrichtigungen (bereits gelesen / noch nicht gelesen), Status der Spalten in Tabellen (Eingeblendet / Ausgeblendet), Fortschritt des Trainingsmodus. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center 14 Web Console ein.

- Kaspersky-Ereignisprotokoll für die Komponenten von Kaspersky Security Center Linux und das durch Kaspersky verwaltete Programm. Das Ereignisprotokoll "Kaspersky" wird auf jedem Gerät gespeichert und nie zum Administrationsserver übertragen.

- Zertifikat für eine sichere Verbindung verwalteter Geräte mit den Komponenten von Kaspersky Security Center Linux. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center 14 Web Console ein.

- Die Administrationsserver-Daten, die der Benutzer in Kaspersky Security Center 14 Web Console eingibt.

- Alle Daten, die der Benutzer auf der Benutzeroberfläche von Kaspersky Security Center 14 Web Console eingibt.

Die oben aufgeführten Daten können in Kaspersky Security Center Linux vorhanden sein, wenn eine der folgenden Methoden verwendet wird:

- Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center 14 Web Console ein.

- Der Administrationsagent empfängt Daten automatisch vom Gerät und überträgt diese an den Administrationsserver.

- Der Administrationsagent empfängt von dem durch Kaspersky verwalteten Programm abgerufenen Daten und überträgt sie an den Administrationsserver. Die Liste der verarbeiteten Daten von den durch Kaspersky verwalteten Programmen finden Sie in der Hilfe der entsprechenden Programme.

- Administrationsserver und Administrationsagenten, denen ein Verteilungspunkt zugeordnet wurde, rufen Informationen über die durch das Netzwerk verbundenen Geräte ab.

Die aufgelisteten Daten werden in der Datenbank des Administrationsservers gespeichert. Benutzernamen und Kennwörter werden in verschlüsselter Form gespeichert.

Alle lokal verarbeiteten Daten, einschließlich Protokolldateien, die von Installationsprogrammen und Dienstprogrammen erstellt wurden, können nur mittels Dump-Dateien, Ablaufverfolgungsdateien oder Protokolldateien von Komponenten von Kaspersky Security Center an Kaspersky Linux übertragen werden.

Kaspersky schützt alle erhaltenen Informationen in Übereinstimmung mit den geltenden Gesetzen und geltenden Kaspersky-Regeln. Daten werden über einen sicheren Kanal übertragen.

Durch folgen der Links in der Verwaltungskonsole oder der Kaspersky Security Center 14 Web Console stimmt der Nutzer zu, die folgenden Daten automatisch zu übertragen:

- Code von Kaspersky Security Center Linux

- Version von Kaspersky Security Center Linux

- Lokalisierung von Kaspersky Security Center Linux

- Lizenz-ID

- Lizenztyp

- Ob die Lizenz über einen Partner bezogen wurde

Die Liste an Daten, die über einen Link zur Verfügung gestellt werden, ist abhängig von Zweck und Standort des Links.

Kaspersky verwendet die erhaltenen Daten in anonymisierter Form und nur für allgemeine Statistiken. Zusammenfassende Statistiken werden automatisch aus den ursprünglich erhaltenen Informationen erstellt und enthalten keine persönlichen oder vertraulichen Daten. Sobald neue Daten akkumuliert wurden, werden die vorherigen Daten gelöscht (einmal pro Jahr). Zusammenfassende Statistiken werden unbegrenzt gespeichert.

Über das Abonnement

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

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

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

Um Kaspersky Security Center Linux 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 Linux verwenden, wenn das Abonnement zuvor abgelaufen ist oder gekündigt wurde.

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

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

Bei einer Nutzung des Programms im Abonnement stellt Kaspersky Security Center Linux zum festgelegten Zeitpunkt vor Ablauf des Abonnements automatisch eine Verbindung zum Aktivierungsserver her. Sie können das Abonnement auf der Website des Providers verlängern.

Ereignisse bei Überschreitung der Lizenzbeschränkung

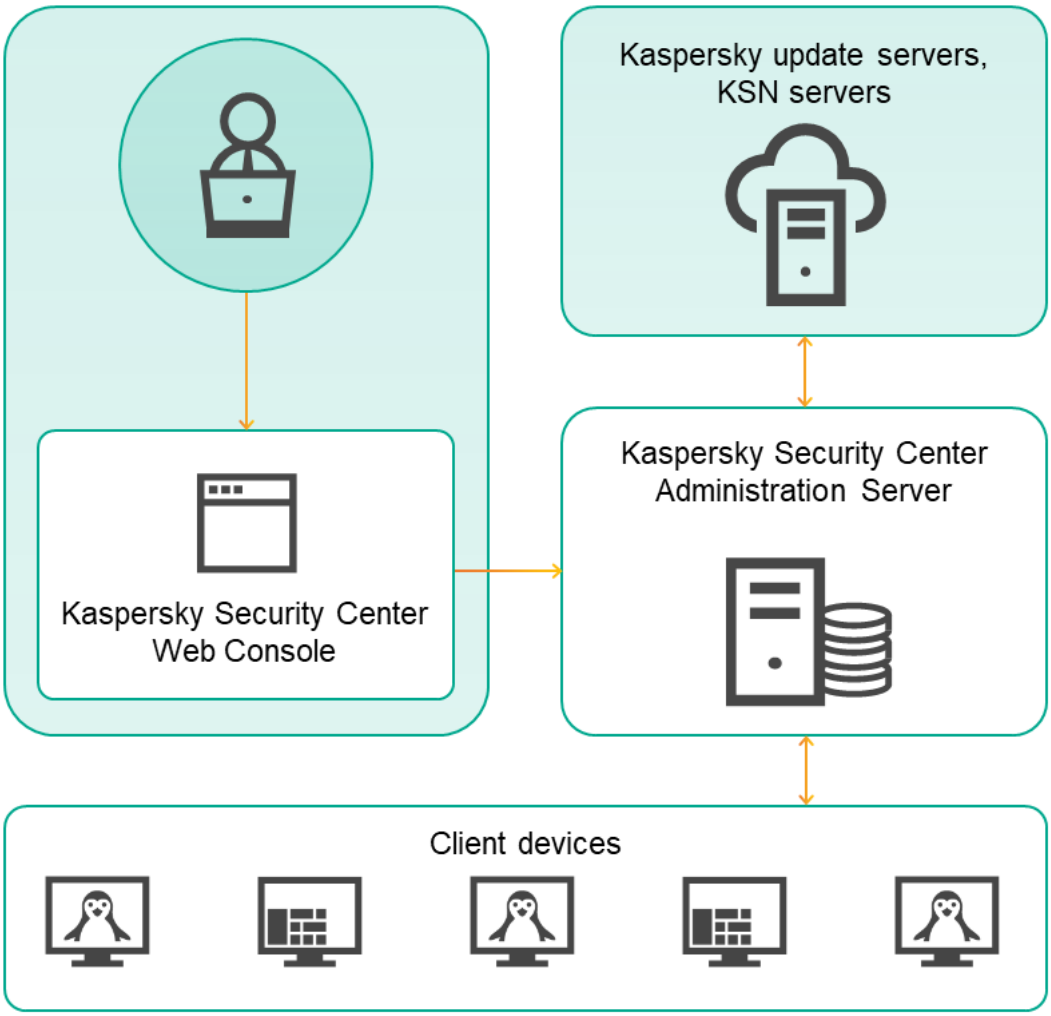
Kaspersky Security Center Linux ermöglicht das automatische Empfangen von Informationen über Ereignisse der Überschreitung der Lizenzbeschränkung von Kaspersky-Programmen, die auf den Client-Geräten installiert sind.

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.

Architektur

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



Architektur von Kaspersky Security Center 14 Linux

Kaspersky Security Center 14 Linux umfasst die folgenden Hauptkomponenten:

- **Kaspersky Security Center Web Console**. Bietet eine Weboberfläche zum Erstellen und Verwalten des Schutzsystems in dem von Kaspersky Security Center verwalteten Netzwerk des Kundenunternehmens.
- **Kaspersky Security Center Administrationsserver** (auch als *Server* bezeichnet). Führt die Funktionen zum zentralen Speichern von Daten über die im Firmennetzwerk installierten Programme und deren Verwaltung aus.
- **Kaspersky-Update-Server**. HTTP(S)-Server bei Kaspersky, von denen Programme von Kaspersky Updates für Datenbanken und Programm-Module herunterladen.
- **KSN-Server**. Server, die eine Datenbank von Kaspersky mit ständig aktualisierten Informationen über die Reputation von Dateien, Web-Ressourcen und Software umfassen. Kaspersky Security Network gewährleistet eine höhere Reaktionsschnelligkeit der Programme von Kaspersky auf Bedrohungen, erhöht die Leistungsfähigkeit einiger Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen.
- **Client-Geräte**. Von Kaspersky Security Center 14 Linux geschützte Geräte eines Kundenunternehmens. Auf jedem zu schützenden Gerät muss eine der Kaspersky-Sicherheits-Apps installiert sein.

Diagramm der Softwareverteilung für Kaspersky Security Center Administrationsserver und Kaspersky Security Center 14 Web Console

Die nachfolgende Abbildung zeigt das Diagramm der Softwareverteilung für Kaspersky Security Center Administrationsserver und Kaspersky Security Center 14 Web Console.

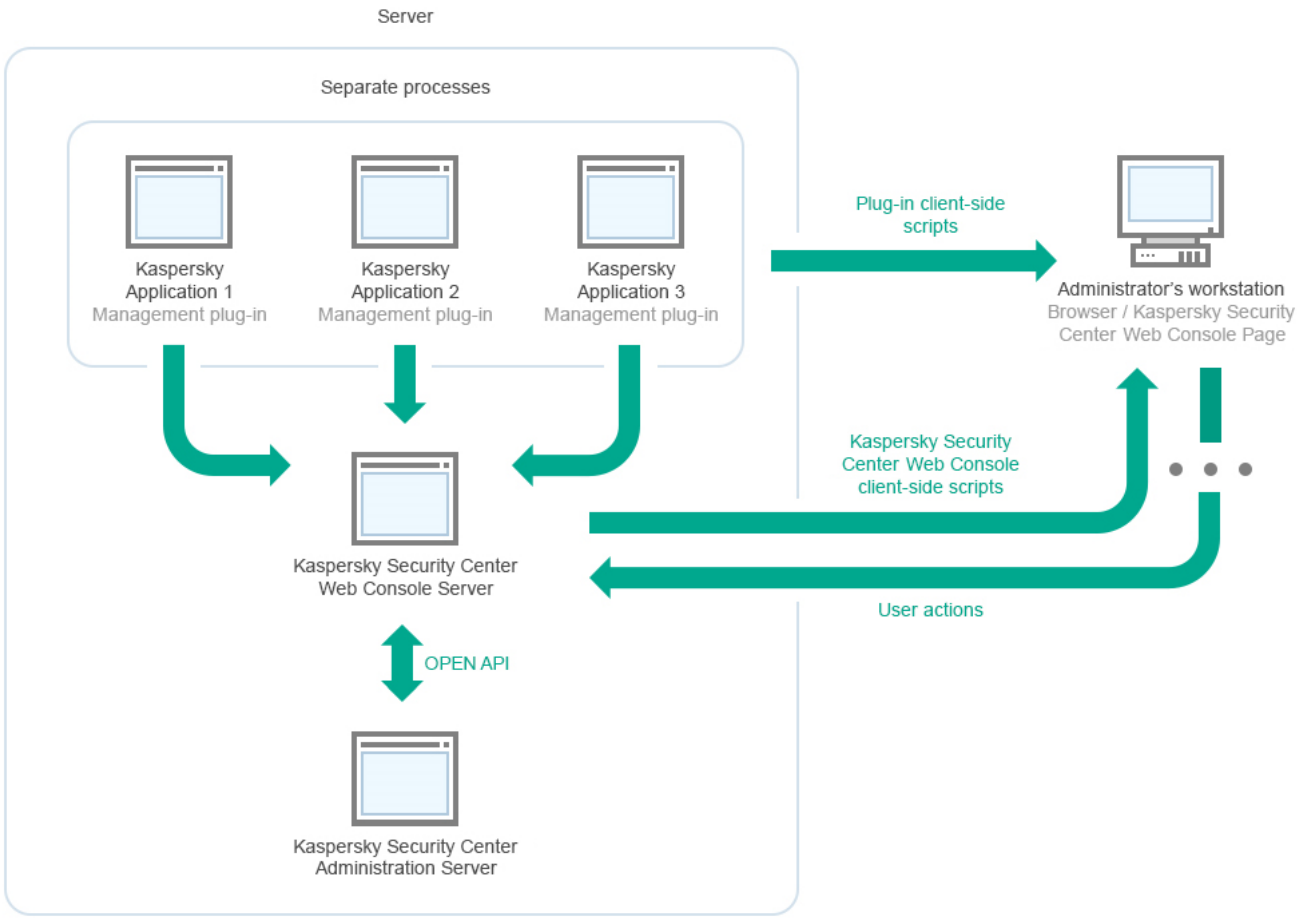


Diagramm der Softwareverteilung für Kaspersky Security Center Administrationsserver und Kaspersky Security Center 14 Web Console

Verwaltungs-Plug-ins für Anwendung von Kaspersky, die auf geschützten Geräten installiert sind (ein Plug-in für jede Anwendung) werden gemeinsam mit Kaspersky Security Center 14 Web Console verteilt.

Als Administrator greifen Sie mittels eines Browsers auf Ihrer Arbeitsstation auf Kaspersky Security Center 14 Web Console zu.

Wenn Sie bestimmte Aktionen in Kaspersky Security Center 14 Web Console durchführen kommuniziert der Server von Kaspersky Security Center 14 Web Console mit dem Kaspersky Security Center Administrationsserver über OpenAPI. Der Server von Kaspersky Security Center 14 Web Console fordert die gewünschten Informationen vom Kaspersky Security Center Administrationsserver an und zeigt die Ergebnisse Ihrer Vorgänge in Kaspersky Security Center 14 Web Console an.

Ports, die von Kaspersky Security Center Linux verwendet werden

Die nachfolgenden Tabellen enthalten die standardmäßigen Ports, die auf dem Administrationsserver und auf den Client-Geräten geöffnet sein müssen. Bei Bedarf können Sie jede dieser standardmäßigen Portnummern ändern.

Ports, die von Kaspersky Security Center Linux Administrationsserver verwendet werden

Port	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
8060	klcsweb	TCP	Weitergabe der veröffentlichten Installationspakete an Client-Geräte	Installationspakete veröffentlichen. Sie können die standardmäßige Portnummer im Abschnitt **Webserver** im Eigenschaftenfenster des Administrationsservers ändern.
8061	klcsweb	TCP (TLS)	Weitergabe der veröffentlichten Installationspakete an Client-Geräte	Installationspakete veröffentlichen. Sie können die standardmäßige Portnummer im Abschnitt **Webserver** im Eigenschaftenfenster des Administrationsservers ändern.
13000	klserver	TCP (TLS)	Aufnahme der Verbindungen von Administrationsagenten und sekundären Administrationsservern; wird auch auf den sekundären Servern für die Aufnahme der Verbindungen vom primären Administrationsserver verwendet (beispielsweise wenn sich der sekundäre Server in einer DMZ befindet)	Verwaltung von Client-Geräten und sekundären Administrationsservern. Sie können die Nummer des standardmäßigen Ports für den Empfang von Verbindungen von Administrationsagenten ändern, wenn Sie während der Installation von Kaspersky Security Center Linux die Verbindungsports konfigurieren. Sie können die Nummer des standardmäßigen Ports für den Empfang von Verbindungen von sekundären Administrationsservern ändern, wenn Sie eine Hierarchie von Administrationsservern erstellen.
13000	klserver	UDP	Annahme der Informationen von Administrationsagenten über das Deaktivieren von Geräten	Verwaltung der Client-Geräte. Sie können die standardmäßige Portnummer in den Richtlinieneinstellungen des Administrationsagenten ändern.
13299	klserver	TCP (TLS)	Aufbau von Verbindungen von der Kaspersky Security Center 14 Web Console zum Administrationsserver; Aufbau von Verbindungen mit dem Administrationsserver über OpenAPI	Kaspersky Security Center 14 Web Console, OpenAPI. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers ändern (im Unterabschnitt **Verbindungsports** des Abschnitts **Allgemein**) oder, wenn Sie eine Hierarchie von Administrationsservern erstellen.
14000	klserver	TCP	Annahme der Verbindungen von den Administrationsagenten	Verwaltung der Client-Geräte.

				Sie können die standardmäßige Portnummer ändern, wenn Sie während der Installation von Kaspersky Security Center Linux die Verbindungsports konfigurieren oder wenn Sie ein Client-Gerät manuell mit dem Administrationsserver verbinden.
13111 (nur, wenn der KSN Proxy-Service auf dem Gerät ausgeführt wird)	ksnproxy	TCP	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers ändern.
15111 (nur, wenn der KSN Proxy-Service auf dem Gerät ausgeführt wird)	ksnproxy	UDP	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers ändern.
17000	klactprx	TCP (TLS)	Annahme der Verbindungen zur Programmaktivierung auf verwalteten Geräten	Proxyserver zur Aktivierung von verwalteten Geräten. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers ändern (im Unterabschnitt **Zusätzliche Ports** des Abschnitts **Allgemein**).
19170	klserver	HTTPS (TLS)	Tunneln der Verbindungen mit verwalteten Geräten mittels "klsctunnel"-Dienstprogramm	Remote-Verbindungen mit verwalteten Geräten mittels Kaspersky Security Center 14 Web Console. Sie können die standardmäßige Portnummer mit dem Dienstprogramm klscflag ändern.

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

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

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

Port	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
8080	Node.js:	TCP	Empfangen	Kaspersky Security Center 14 Web Console.

	Serverseitiges JavaScript	(TLS)	von Verbindungen vom Webbrowser zur Kaspersky Security Center 14 Web Console	Sie können die standardmäßige Portnummer ändern, wenn Sie Kaspersky Security Center 14 Web Console installieren. Wenn Sie die Kaspersky Security Center 14 Web Console auf dem ALT Linux-Betriebssystem installieren, müssen Sie eine andere Portnummer als 8080 angeben, da Port 8080 von dem Betriebssystem verwendet wird.

Die folgende Tabelle zeigt den Port, der auf verwalteten Geräten mit installiertem Administrationsagent geöffnet sein muss.

Ports, die vom Administrationsagenten verwendet werden

Port	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
15000	klnagent	UDP	Verwaltungssignale vom Administrationsserver an die Administrationsagenten	Verwaltung der Client-Geräte. Sie können die standardmäßige Portnummer in den Richtlinieneinstellungen des Administrationsagenten ändern.
15000	klnagent	UDP-Broadcast	Abrufen von Daten über andere Administrationsagenten in derselben Broadcast-Domäne (die Daten werden dann an den Administrationsserver gesendet)	Zustellung von Updates und Installationspaketen.
15001	klnagent	UDP	Empfangen von Multicast-Anfragen von einem Verteilungspunkt (falls verwendet)	Empfang von Updates und Installationspaketen von einem Verteilungspunkt. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Verteilungspunkts ändern.

Die nachfolgende Tabelle zeigt die Ports, die auf einem verwalteten Gerät mit installiertem Administrationsagenten, welcher als Verteilungspunkt fungiert, geöffnet sein müssen. Die aufgelisteten Ports müssen auf den Verteilungspunkt-Geräten zusätzlich zu den von Administrationsagenten verwendeten Ports geöffnet sein (siehe Tabelle oben).

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

Port	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
13000	klnagent	TCP (TLS)	Annahme der Verbindungen von den Administrationsagenten	Verwaltung von Client-Geräten, Zustellung von Updates und Installationspaketen.

				Sie können die standardmäßige Portnummer in den Eigenschaften des Verteilungspunkts ändern.
13111 (nur, wenn der KSN Proxy-Service auf dem Gerät ausgeführt wird)	ksnproxy	TCP	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver. Sie können die standardmäßige Portnummer in den Eigenschaften des Verteilungspunkts ändern.
15111 (nur, wenn der KSN Proxy-Service auf dem Gerät ausgeführt wird)	ksnproxy	UDP	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver. Sie können die standardmäßige Portnummer in den Eigenschaften des Verteilungspunkts ändern.

Von Kaspersky Security Center 14 Web Console verwendete Ports

Die untenstehende Tabelle listet alle Ports auf, die auf dem Gerät geöffnet werden müssen, auf dem Kaspersky Security Center 14 Web Console Server (auch Kaspersky Security Center 14 Web Console genannt) installiert ist.

Von Kaspersky Security Center 14 Web Console verwendete Ports

Port	Name des Dienstes	Protokoll	Zweck des Ports	Gültigkei
2001	KSCWebConsolePlugin	HTTPS	API-Port, der von den Prozessen der Verwaltungs-Plug-ins verwendet wird, um Anfragen des Dienstes KSCWebConsoleManagementService zu empfangen	Ausführe node.exe Prozesse Verwaltu Plug-ins
1329, 2003	KSCWebConsoleManagementService	HTTPS	API-Ports, die verwendet werden, um Anfragen von dem auf dem gleichen Gerät ausgeführten Dienst KSCWebConsole zu empfangen	Aktualisie Kompone Kaspersk Security 14 Web C
2005	KSCWebConsole	HTTPS	API-Port, der verwendet wird, um Anfragen von dem auf dem gleichen Gerät ausgeführten KSCWebConsoleManagementService-Dienst zu empfangen	Ausführe node.exe Prozesse Kaspersk Security 14 Web C
8200	–	HTTP	API-Port, der für die Erstellung von Zertifikaten unter Verwendung von HashiCorp Vault verwendet wird (Weitere Informationen entnehmen Sie der Website von HashiCorp Vault)	Installiere Kaspersk Security 14 Web C und Aktu der Komp von Kasp Security 14 Web C
4150, 4151, 4152	KSCWebConsoleMessageQueue	HTTPS	API-Ports des Message Brokers, die für die Kommunikation zwischen den Prozessen von Kaspersky Security Center Web Console 14 und den Verwaltungs-Plug-ins verwendet werden	Interaktio zwischen Kaspersk Security 14 Web C und Verw Plug-ins

Installation

Dieser Abschnitt beschreibt die Installation für Kaspersky Security Center und Kaspersky Security Center 14 Web Console.

Hauptinstallationsszenario

Nach diesem Szenario können Sie den Kaspersky Security Center 14 Linux Administrationsserver und Kaspersky Security Center 14 Web Console installieren, mithilfe des Schnellstartassistenten die Ersteinrichtung des Administrationsservers durchführen und mithilfe des Assistenten für die Bereitstellung des Schutzes Kaspersky-Apps auf den verwalteten Geräten installieren.

Erforderliche Maßnahmen

Sie müssen einen Lizenzschlüssel (Aktivierungscode) für Kaspersky Endpoint Security for Business oder Lizenzschlüssel (Aktivierungscodes) für Kaspersky-Sicherheits-Apps haben.

Wenn Sie Kaspersky Security Center 14 Linux zuerst ausprobieren möchten, können Sie von der Kaspersky-Website eine kostenlose 30-Tage-Testversion herunterladen.

Schritte

Das Hauptinstallationsszenario besteht aus den folgenden Schritten:

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

   Erfahren Sie mehr über die Komponenten von Kaspersky Security Center Linux. Bestimmen Sie ausgehend von der Konfiguration des Netzwerks und der Bandbreite der Übertragungskanäle, wie viele Administrationsserver verwendet und wie sie über Ihre Büros verteilt werden sollen (sofern Sie ein verteiltes Netzwerk verwenden).

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

2. **Vorbereitung der Verwendung benutzerdefinierter Zertifikate**

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

3. **Installation eines Datenbank-Managementsystems (DBMS)**

   Installation des Datenbank-Managementsystems (DBMS) oder eines anderen Systems, das von Kaspersky Security Center verwendet werden soll.

4. **Konfiguration der Ports**

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

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

5. **Kaspersky Security Center installieren**

   Wählen Sie ein Linux-Gerät aus, das Sie als Administrationsserver verwenden möchten, stellen Sie sicher, dass das Gerät die Software- und Hardwareanforderungen erfüllt, und installieren Sie dann Kaspersky Security Center auf dem Gerät. Die Serverversion des Administrationsagenten wird zusammen mit dem Administrationsserver installiert.

6. **Kaspersky Security Center 14 Web Console und Verwaltungs-Web-Plug-ins installieren**

   Wählen Sie ein Linux-Gerät aus, das Sie als Administrator-Arbeitsplatz verwenden möchten, stellen Sie sicher, dass das Gerät die Software- und Hardwareanforderungen erfüllt, und installieren Sie dann Kaspersky Security Center 14 Web Console auf dem Gerät. Sie können Kaspersky Security Center 14 Web Console entweder auf demselben Gerät installieren, auf dem der Administrationsserver installiert ist, oder auf einem anderen Gerät.

   Laden Sie das Verwaltungs-Web-Plug-in für Kaspersky Endpoint Security für Linux herunter und installieren Sie es dann auf demselben Gerät, auf dem Kaspersky Security Center 14 Web Console installiert ist.

7. **Kaspersky Endpoint Security für Linux und den Administrationsagenten auf dem Gerät mit dem Administrationsserver installieren**

   Standardmäßig betrachtet das Programm das Gerät mit dem Administrationsserver nicht als verwaltetes Gerät. Um den Administrationsserver vor Viren und anderen Bedrohungen zu schützen und das Gerät wie alle anderen verwalteten Geräte zu verwalten, empfehlen wir Ihnen, Kaspersky Endpoint Security für Linux und den Administrationsagenten für Linux auf dem Gerät des Administrationsservers zu installieren. In diesem Fall wird der Administrationsagent für Linux installiert und funktioniert unabhängig von der Serverversion des Administrationsagenten, die Sie zusammen mit dem Administrationsserver installiert haben.

8. **Erstkonfiguration vornehmen**

   Nach Abschluss der Installation des Administrationsservers wird bei der ersten Verbindung mit dem Administrationsserver automatisch der Schnellstartassistent ausgeführt. Befolgen Sie die Schritte des Assistenten, um die Erstkonfiguration des Administrationsservers nach Bedarf vorzunehmen. Während der Erstkonfiguration erstellt der Assistent die zur Bereitstellung des Schutzes notwendigen Richtlinien und Aufgaben mit Standardeinstellungen. Diese Einstellungen sind eventuell nicht optimal für Ihr Unternehmen geeignet. Sie können bei Bedarf die Einstellungen der Richtlinien und Aufgaben ändern.

9. **Suche der Geräte im Netzwerk**

   Ermitteln Sie die Geräte manuell. Daraufhin erhält Kaspersky Security Center Linux die Adressen und die Namen aller Geräte, die im Netzwerk registriert sind. Anschließend können Sie Kaspersky Security Center Linux verwenden, um Apps von Kaspersky und von anderen Herstellern auf den gefundenen Geräten zu installieren. Da Kaspersky Security Center Linux die Gerätesuche regelmäßig startet, werden neue Geräte im Netzwerk automatisch gefunden, sobald sie auftauchen.

10. **Geräte in Administrationsgruppen anordnen**

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

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

11. **Verteilungspunkte zuweisen**

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

12. **Installation des Administrationsagenten und der Sicherheitsanwendungen auf den Geräten im Netzwerk**

Als Bereitstellung des Schutzes in einem Unternehmensnetzwerk wird die Installation von Administrationsagenten und Sicherheitsprogrammen auf den Geräten verstanden, die vom Administrationsserver bei der Gerätesuche im Unternehmensnetzwerk gefunden wurden.

Um die Anwendungen remote zu installieren, führen Sie den Assistenten für die Bereitstellung des Schutzes aus.

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

Bevor Sie den Administrationsagenten und die Sicherheitsanwendung auf Geräten im Netzwerk installieren, stellen Sie sicher, dass diese Geräte verfügbar (aktiviert) sind.

13. **Lizenzschlüssel auf Client-Geräte verteilen**

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

14. **Konfigurieren von Richtlinien für Kaspersky-Anwendungen**

    Um verschiedene Programmeinstellungen auf verschiedene Geräte anzuwenden, können Sie eine geräteorientierte Sicherheitsverwaltung und/oder eine benutzerorientierte Sicherheitsverwaltung verwenden. Die geräteorientierte Sicherheitsverwaltung kann über Richtlinien und Aufgaben implementiert werden. Sie können Aufgaben nur auf die Geräte anwenden, die bestimmte Bedingungen erfüllen. Um Bedingungen für das Filtern von Geräten festzulegen, verwenden Sie die Geräteauswahl und Tags.

15. **Überwachen des Netzwerkschutzstatus**

    Sie können Ihr Netzwerk mithilfe von Widgets auf dem Dashboard überwachen, Berichte in Kaspersky-Anwendungen erstellen sowie von Anwendungen auf verwalteten Geräten empfangene Ereignisauswahlen und Benachrichtigungslisten anzeigen.

Installation eines Datenbank-Managementsystems

Installieren Sie das Datenbank-Managementsystem (DBMS), das von Kaspersky Security Center verwendet werden soll. Sie können eine der unterstützten DBMS auswählen.

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

Wenn Sie MariaDB verwenden, müssen Sie die empfohlenen Einstellungen konfigurieren, damit die DBMS optimal mit Kaspersky Security Center funktioniert.

Den MariaDB x64-Server für die Verwendung mit Kaspersky Security Center 14 Linux konfigurieren

Wenn Sie den MariaDB-Server für Kaspersky Security Center verwenden, aktivieren Sie die Unterstützung für InnoDB und MEMORY-Speicher sowie für die Codierungen UTF-8 und UCS-2.

Empfohlene Einstellungen für die Datei my.cnf

Um die Datei my.cnf zu konfigurieren:

1. Öffnen Sie die Datei my.cnf in einem Texteditor.
2. Geben Sie die folgenden Zeilen in die Datei my.cnf ein:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=<Wert>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

Der Wert von `innodb_buffer_pool_size` muss mindestens 80 Prozent der erwarteten KAV-Datenbankgröße betragen.

Es wird empfohlen, den Parameterwert `innodb_flush_log_at_trx_commit=0` zu verwenden, da die Werte "1" oder "2" die Geschwindigkeit von MariaDB negativ beeinflussen.

Standardmäßig sind die Optimierungs-Add-ons `join_cache_incremental`, `join_cache_hashed` und `join_cache_bka` aktiviert. Wenn diese Add-ons nicht aktiviert sind, müssen Sie sie aktivieren.

Um zu überprüfen, ob die Optimierungs-Add-ons aktiviert sind:

1. Führen Sie in der MariaDB-Client-Konsole den folgenden Befehl aus:

   ```
   SELECT @@optimizer_switch;
   ```

2. Stellen Sie sicher, dass die Ausgabe die folgenden Zeilen enthält:

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   Wenn diese Zeilen vorhanden sind und die Werte `on` haben, sind die Optimierungs-Add-ons aktiviert.

   Falls diese Zeilen fehlen oder die Werte `off` haben:

   a. Öffnen Sie die Datei my.cnf in einem Texteditor.

   b. Fügen Sie die folgenden Zeilen in die Datei my.cnf ein:

   ```
   optimizer_switch='join_cache_incremental=on'
   optimizer_switch='join_cache_hashed=on'
   optimizer_switch='join_cache_bka=on'
   ```

Die Add-ons `join_cache_incremental`, `join_cache_hash` und `join_cache_bka` sind aktiviert.

Kaspersky Security Center installieren

In diesem Ablauf wird beschrieben, wie Kaspersky Security Center installiert wird.

Vor der Installation:

- Installieren Sie ein Datenbank-Managementsystem.

- Stellen Sie sicher, dass auf dem Gerät, auf dem Sie Kaspersky Security Center installieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.

Verwenden Sie die Installationsdatei ksc64_[Versionsnummer]_amd64.deb oder ksc64-[Versionsnummer].x86_64.rpm, die der auf Ihrem Gerät installierten Linux-Distribution entspricht. Sie erhalten die Installationsdatei, indem Sie sie von der Kaspersky-Website herunterladen.

Um Kaspersky Security Center zu installieren, gehen Sie wie folgt vor:

1. Führen Sie in der Befehlszeile unter einem Benutzerkonto mit Root-Rechten die in dieser Anleitung genannten Befehle aus.

2. Erstellen Sie die Gruppe 'kladmins' und das nicht privilegierte Benutzerkonto 'ksc'. Das Benutzerkonto muss Mitglied der Gruppe 'kladmins' sein. Führen Sie dazu nacheinander die folgenden Befehle aus:
   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```

3. Führen Sie die Installation von Kaspersky Security Center aus. Führen Sie abhängig von Ihrer Linux-Distribution einen der folgenden Befehle aus:

   - `# apt install /<path>/ksc64_[Versionsnummer]_amd64.deb`

   - `# yum install /<path>/ksc64-[Versionsnummer].x86_64.rpm -y`

4. Konfigurieren Sie Kaspersky Security Center:
   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Lesen Sie den Endbenutzer-Lizenzvertrag (EULA) und die Datenschutzrichtlinie. Der Text wird im Befehlszeilenfenster angezeigt. Drücken Sie die Leertaste, um das nächste Textsegment anzuzeigen. Geben Sie nach der entsprechenden Aufforderung die folgenden Werte ein:

   a. Geben Sie `y` ein, wenn Sie die EULA-Bedingungen verstehen und akzeptieren. Geben Sie `n` ein, wenn Sie den EULA-Bedingungen nicht zustimmen. Um Kaspersky Security Center zu nutzen, müssen Sie den Bestimmungen des Endbenutzer-Lizenzvertrags (EULA) zustimmen.

   b. Geben Sie `y` ein, wenn Sie die Bedingungen der Datenschutzrichtlinie verstehen und akzeptieren, und Sie damit einverstanden sind, dass Ihre Daten so verarbeitet und (einschließlich in Drittländer) übertragen werden, wie es in der Datenschutzrichtlinie beschrieben ist. Geben Sie `n` ein, wenn Sie den Bedingungen der Datenschutzrichtlinie nicht zustimmen. Um Kaspersky Security Center zu nutzen, müssen Sie den Bestimmungen der Datenschutzrichtlinie zustimmen.

6. Geben Sie nach der entsprechenden Aufforderung die folgenden Einstellungen ein:

   a. Geben Sie den DNS-Namen oder die statische IP-Adresse des Administrationsservers ein.

   b. Geben Sie die Portnummer des Administrationsservers ein. Standardmäßig ist die Portnummer 14000 festgelegt.

   c. Geben Sie die SSL-Portnummer des Administrationsservers ein. Standardmäßig ist die Portnummer 13000 festgelegt.

   d. Ermitteln Sie die ungefähre Anzahl der Geräte, die Sie verwalten möchten:

      - Geben Sie für 1 bis 100 vernetzte Geräte den Wert 1 ein.

- Geben Sie für 101 bis 1.000 vernetzte Geräte den Wert 2 ein.
- Geben Sie für über 1.000 vernetzte Geräte den Wert 3 ein.

e. Geben Sie den Namen der Sicherheitsgruppe für Dienste ein. Standardmäßig wird die Gruppe 'kladmins' verwendet.

f. Geben Sie den Namen des Benutzerkontos ein, um den Administrationsserver-Dienst zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein. Standardmäßig wird das Konto 'ksc' verwendet.

g. Geben Sie den Namen des Benutzerkontos ein, um andere Dienste zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein. Standardmäßig wird das Konto 'ksc' verwendet.

h. Geben Sie die IP-Adresse des Gerätes ein, auf dem die Datenbank installiert ist.

i. Geben Sie die Portnummer der Datenbank ein. Dieser Port wird für die Kommunikation mit dem Administrationsserver verwendet. Standardmäßig ist die Portnummer 3306 festgelegt.

j. Geben Sie den Namen der Datenbank ein.

k. Geben Sie den Benutzernamen des Datenbank-Root-Benutzerkontos ein, das Sie für den Zugriff auf die Datenbank verwenden.

l. Geben Sie das Kennwort des Datenbank-Root-Benutzerkontos ein, das Sie für den Zugriff auf die Datenbank verwenden.

   Warten Sie, bis die Dienste hinzugefügt und automatisch gestartet wurden:

   - `klnagent_srv`
   - `kladminserver_srv`
   - `klactprx_srv`
   - `klwebsrv_srv`

m. Erstellen Sie ein Benutzerkonto, das als Administrator des Administrationsservers fungiert. Geben Sie den Benutzernamen und das Kennwort ein.

   Das Kennwort muss den folgenden Regeln entsprechen:

   - Das Benutzerkennwort muss mindestens 8 Zeichen und darf maximal 16 Zeichen enthalten.
   - Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Gruppen enthalten:
     - Großbuchstaben (A–Z)
     - Kleinbuchstaben (a–z)
     - Zahlen (0–9)
     - Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Der Benutzer wird hinzugefügt und Kaspersky Security Center wird installiert.

Überprüfung von Diensten

Verwenden Sie die folgenden Befehle, um zu überprüfen, ob ein Dienst ausgeführt wird oder nicht:

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

Kaspersky Security Center 14 Web Console installieren

In diesem Abschnitt wird beschrieben, wie Sie den Kaspersky Security Center 14 Web Console Server (auch als Kaspersky Security Center 14 Web Console bezeichnet) auf Geräten mit Linux-Betriebssystemen installieren. Vor der Installation müssen Sie ein Datenbank-Managementsystem und den Kaspersky Security Center Administrationsserver installieren.

Verwenden Sie eine der folgenden Installationsdateien, die der auf Ihrem Gerät installierten Linux-Distribution entspricht:

- Für Debian – ksc-web-console-[Build-Nummer].x86_64.deb
- Für RPM-basierte Betriebssysteme – ksc-web-console-[Build-Nummer].x86_64.rpm
- Für Alt 8 SP – ksc-web-console-[Build-Nummer]-alt8p.x86_64.rpm

Sie erhalten die Installationsdatei, indem Sie sie von der Kaspersky-Website herunterladen.

Um Kaspersky Security Center 14 Web Console zu installieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass auf dem Gerät, auf dem Sie Kaspersky Security Center 14 Web Console installieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.
2. Lesen Sie den Endbenutzer-Lizenzvertrag (EULA) im Installationspaket (Datei /var/opt/kaspersky/ksc-web-console/license-<XX>.txt, wobei <XX> für einen Sprachcode steht). Falls Sie den Lizenzvertrag ablehnen, installieren Sie die Anwendung nicht.
3. Erstellen Sie eine Antwortdatei mit Parametern für die Verbindung zwischen Kaspersky Security Center 14 Web Console und dem Administrationsserver. Nennen Sie die Datei "ksc-web-console-setup.json" und platzieren Sie diese in dem folgenden Pfad: /etc/ksc-web-console-setup.json.

   Beispiel für eine Antwortdatei mit minimalem Parametersatz sowie Standardadresse und Standardport:

   ```
   {
     "address": "127.0.0.1",
     "port": "8080",
     "trusted":
   "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
   Server",
     "acceptEula": "true"
   }
   ```

   Wenn Sie die Kaspersky Security Center 14 Web Console auf dem Betriebssystem ALT Linux installieren, müssen Sie eine andere Portnummer als 8080 angeben, da Port 8080 vom Betriebssystem verwendet wird.

Kaspersky Security Center 14 Web Console kann nicht aktualisiert werden, wenn dafür die gleiche rpm-Installationsdatei verwendet wird. Wenn Sie die Einstellungen in einer Antwortdatei ändern und diese Datei zur Neuinstallation der Anwendung verwenden möchten, müssen Sie die Anwendung zunächst löschen und sie anschließend mit der neuen Antwortdatei erneut installieren.

4. Führen Sie unter einem Konto mit Root-Berechtigungen mithilfe der Befehlszeile und abhängig von Ihrer Linux-Distribution die Setup-Datei mit der Erweiterung .deb oder .rpm aus.

   - Um Kaspersky Security Center 14 Web Console aus einer .deb-Datei zu installieren oder zu aktualisieren, führen Sie den folgenden Befehl aus:
     ```
     $ sudo dpkg -i ksc-web-console-[Build-Nummer].x86_64.deb
     ```
   - Um Kaspersky Security Center 14 Web Console aus einer .rpm -Datei zu installieren, führen Sie einen der folgenden Befehl aus:
     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-[Build-Nummer].x86_64.rpm
     ```
     oder
     ```
     $ sudo alien -i ksc-web-console-[Build-Nummer].x86_64.rpm
     ```
   - Um von einer früheren Version von Kaspersky Security Center Web Console zu aktualisieren, führen Sie einen der folgenden Befehle aus:
     - Für Geräte mit RPM-basiertem Betriebssystem:
       ```
       $ sudo rpm -Uvh --nodeps --force ksc-web-console-[Build-Nummer].x86_64.rpm
       ```
     - Für Geräte mit Debian-basiertem Betriebssystem:
       ```
       $ sudo dpkg -i ksc-web-console-[Build-Nummer].x86_64.deb
       ```

   Dadurch wird die Setup-Datei entpackt. Bitte warten Sie, bis die Installation abgeschlossen ist. Kaspersky Security Center 14 Web Console wird in den folgenden Pfad installiert: /var/opt/kaspersky/ksc-web-console.

5. Starten Sie alle Dienste von Kaspersky Security Center 14 Web Console neu, indem Sie den folgenden Befehl ausführen:
   ```
   $ sudo systemctl restart KSC*
   ```

Nach dem erfolgreichen Abschluss der Installation können Sie in Ihrem Browser Kaspersky Security Center 14 Web Console öffnen und sich einloggen.

Installationsparameter für Kaspersky Security Center 14 Web Console

Für die Installation von Kaspersky Security Center 14 Web Console Server auf Linux-Geräten, müssen Sie eine Antwortdatei erstellen. Dies muss eine .json-Datei sein, die die Parameter für die Verbindung von Kaspersky Security Center 14 Web Console mit dem Administrationsserver enthält.

Hier ist ein Beispiel für eine Antwortdatei mit dem minimalem Parametersatz sowie Standardadresse und Standardport:

```
{
  "address": "127.0.0.1",
  "port": "8080",
  "defaultLangId": 1049,
  "enableLog": false,
```

```
  "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
Server",
  "acceptEula": true,
  "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
  "webConsoleAccount": "Group1:User1",
  "managementServiceAccount": "Group1:User2",
  "serviceWebConsoleAccount": "Group1:User3",
  "pluginAccount": "Group1:User4",
  "messageQueueAccount": "Group1:User5"
}
```

Wenn Sie die Kaspersky Security Center 14 Web Console auf dem ALT Linux-Betriebssystem installieren, müssen Sie eine andere Portnummer als 8080 angeben, da Port 8080 von dem Betriebssystem verwendet wird.

In der folgenden Tabelle werden die Parameter beschrieben, die in einer Antwortdatei angegeben werden können.

Parameter für die Installation von Kaspersky Security Center 14 Web Console auf Geräten mit Linux

Parameter	Beschreibung	Mögliche We
`Adresse`	Serveradresse der Kaspersky Security Center 14 Web Console (erforderlich).	Zeichenfolgenwert.
`Port`	Nummer des Ports, über den der Server der Kaspersky Security Center 14 Web Console eine Verbindung zum Administrationsserver herstellt (erforderlich).	Zahlenwert.
`defaultLangId`	Sprache der Benutzeroberfläche (standardmäßig `1033`).	Zahlencodes der Sprachen: • Deutsch: `1031` • Englisch: `1033` • Spanisch: `3082` • Spanisch (Mexiko): `2058` • Französisch: `1036` • Japanisch: `1041` • Kasachisch: `1087` • Polnisch: `1045` • Portugiesisch (Brasilien): `1046` • Russisch: `1049` • Türkisch: `1055` • Vereinfachtes Chinesisch: `4`

		• Traditionelles Chinesisch: `31748` Wenn kein Wert angegeben ist, wird Englis
`enableLog`	Gibt an, ob die Aktivitätsprotokollierung in Kaspersky Security Center 14 Web Console aktiviert werden soll oder nicht.	Boolescher Wert: • `true` – Protokollierung aktiviert (stand • `false` – Protokollierung deaktiviert.
`Vertrauenswürdig`	Liste der vertrauenswürdigen Administrationsserver, die zur Verbindung mit Kaspersky Security Center 14 Web Console berechtigt sind. Für jeden Administrationsserver müssen die folgenden Parameter definiert sein: • Adresse des Administrationsservers • OpenAPI-Port, der von Kaspersky Security Center 14 Web Console zur Verbindung mit dem Administrationsserver genutzt wird (standardmäßig 13299) • Pfad zum Zertifikat des Administrationsservers • Der im Login-Fenster anzuzeigende Name des Administrationsservers Die Parameter werden durch senkrechte Striche separiert. Wenn mehrere Administrationsserver angegebenen werden, separieren Sie diese durch zwei senkrechte Striche (Pipes).	Zeichenkette im folgenden Format: `"Serveradresse|Port|Pfad zum Zer` Beispiel: `X.X.X.X|13299|/cert/server-1.cer|Server 1||Y.Y.Y.Y|13299|/c 2.cer|Server 2`.
`acceptEula`	Gibt an, ob Sie die Bedingungen des Endbenutzer-Lizenzvertrags (EULA) akzeptieren oder nicht. Die Datei mit den Bedingungen des Endbenutzer-Lizenzvertrags (EULA) wird zusammen mit der Installationsdatei heruntergeladen.	Boolescher Wert: • `true` – Ich habe die Bedingungen des vollständig gelesen, und verstehe und • `false` – Ich lehne die Bedingungen de (standardmäßig ausgewählt).
`certDomain`	Wenn Sie ein neues Zertifikat generieren möchten, können Sie mithilfe dieses Parameters den Domänennamen angeben, für den das Zertifikat generiert werden soll.	Zeichenfolgenwert.

`certPath`	Wenn Sie ein bestehendes Zertifikat verwenden möchten, können Sie mithilfe dieses Parameters den Pfad zur Zertifikatsdatei angeben.	Zeichenfolgenwert. Geben Sie den Pfad `"/var/opt/kaspersky/klnagent_srv` an, um das vorhandene Zertifikat zu verwe benutzerdefiniertes Zertifikat den Speich benutzerdefinierten Zertifikats an.
`keyPath`	Wenn Sie ein bestehendes Zertifikat verwenden möchten, können Sie mithilfe dieses Parameters den Pfad zur KEY-Zertifikatsdatei angeben.	Zeichenfolgenwert.
`webConsoleAccount`	Name des Benutzerkontos, unter dem der Dienst KSCWebConsole ausgeführt wird.	Zeichenkette im folgenden Format: `"Grup` Beispiel: `"Gruppe1:Benutzer1"`. Wenn kein Wert angegeben wird, erstellt Kaspersky Security Center 14 Web Conso mit dem Standardnamen `user_manageme`
`managementServiceAccount`	Name des privilegierten Benutzerkontos, unter dem der Dienst KSCWebConsoleManagement ausgeführt wird.	Zeichenkette im folgenden Format: `"Grup` Beispiel: `"Gruppe1:Benutzer1"`. Wenn kein Wert angegeben wird, erstellt Kaspersky Security Center 14 Web Conso mit dem Standardnamen `user_nodejs_`
`serviceWebConsoleAccount`	Name des Benutzerkontos, unter dem der Dienst KSCSvcWebConsole ausgeführt wird.	Zeichenkette im folgenden Format: `"Grup` Beispiel: `"Gruppe1:Benutzer1"`. Wenn kein Wert angegeben wird, erstellt Kaspersky Security Center 14 Web Conso mit dem Standardnamen `user_svc_node`
`pluginAccount`	Name des Benutzerkontos, unter dem der Dienst KSCWebConsolePlugin ausgeführt wird.	Zeichenkette im folgenden Format: `"Grup` Beispiel: `"Gruppe1:Benutzer1"`. Wenn kein Wert angegeben wird, erstellt Kaspersky Security Center 14 Web Conso mit dem Standardnamen `user_web_plug`
`messageQueueAccount`	Name des Benutzerkontos, unter dem der Dienst KSCWebConsoleMessageQueue ausgeführt wird.	Zeichenkette im folgenden Format: `"Grup` Beispiel: `"Gruppe1:Benutzer1"`. Wenn kein Wert angegeben wird, erstellt Kaspersky Security Center 14 Web Conso mit dem Standardnamen `user_message_`

Wenn Sie die Parameter `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` oder `messageQueueAccount` angeben, stellen Sie sicher, dass die benutzerdefinierten Benutzerkonten derselben Sicherheitsgruppe angehören. Wenn diese Parameter nicht angegeben werden, erstellt das Installationsprogramm von Kaspersky Security Center 14 Web Console eine standardmäßige Sicherheitsgruppe und legt anschließend Benutzerkonten mit Standardnamen in dieser Gruppe an.

Benutzerkonten für die Arbeit mit DBMS

Die folgende Tabelle enthält Informationen zu den Eigenschaften von Benutzerkonten, die für die Arbeit mit MariaDB DBMS ausgewählt wurden.

Als *lokales DBMS* wird das DBMS bezeichnet, das auf demselben Gerät installiert ist wie der Administrationsserver. Als *Remote-DBMS* wird das DBMS bezeichnet, das auf einem anderen Gerät installiert ist.

Geben Sie alle Rechte an, die für das Benutzerkonto des Administrationsservers vor dem Start des Dienstes des Administrationsservers benötigt werden.

DBMS: MariaDB

Speicherort des DBMS	Lokal oder Remote.	Lokal oder Remote.
Wer erstellt die KAV-Datenbank	Installationsprogramm (automatisch)	Administrator (manuell)
Benutzerkonto, unter dem der Installer ausgeführt wird	Lokal oder Domäne, mit lokalen Administratorrechten.	Lokal oder Domäne, mit lokalen Administratorrechten.
Benutzerkonto für Dienst des Administrationsservers	Lokal oder Domäne.	Lokal oder Domäne.
Rechte des internen DBMS-Kontos, die vom Installationsprogramm und dem Dienst des Administrationsservers für den Zugriff auf das DBMS verwendet werden	Root-Zugriff ist erforderlich.	`GRANT ALL` für die KAV-Datenbank sowie `SELECT`, `SHOW VIEW` und `PROCESS` für die Systemtabellen.

Bereitstellung des Kaspersky-Failover-Clusters

Dieser Abschnitt enthält sowohl allgemeine Informationen zum Kaspersky-Failover-Cluster als auch Anweisungen zur Vorbereitung und Bereitstellung des Kaspersky-Failover-Clusters in Ihrem Netzwerk.

Szenario: Kaspersky Failover Cluster bereitstellen

Ein Kaspersky-Failover-Cluster bietet eine hohe Verfügbarkeit für Kaspersky Security Center und minimiert die Ausfallzeit des Administrationsservers im Falle eines Fehlers. Das Failover-Cluster basiert auf zwei identischen Instanzen von Kaspersky Security Center, die auf zwei Computern installiert sind. Eine der Instanzen arbeitet als aktiver Knoten und die andere ist ein passiver Knoten. Der aktive Knoten verwaltet den Schutz der Client-Geräte, während der passive bereit ist, alle Funktionen des aktiven Knotens zu übernehmen, falls der aktive Knoten ausfällt. Wenn ein Fehler auftritt, wird der passive Knoten aktiv und der aktive Knoten wird passiv.

Erforderliche Maßnahmen

Sie verfügen über die Hardware, welche die Anforderungen für das Failover Cluster erfüllt.

Die Bereitstellung von Kaspersky-Programmen erfolgt schrittweise:

1. **Erstellen eines Kontos für die Dienste von Kaspersky Security Center**

   Erstellen Sie ein neues Domänenbenutzerkonto oder wählen Sie ein vorhandenes aus, unter dem die Dienste von Kaspersky Security Center ausgeführt werden. Fügen Sie das ausgewählte Benutzerkonto zur Gruppe der lokalen Administratoren auf jedem der Knoten und auf dem Dateiserver hinzu.

2. **Vorbereiten des Dateiservers**

   Bereiten Sie den Dateiserver darauf vor, als Komponente des Kaspersky Failover Clusters zu fungieren. Stellen Sie sicher, dass der Dateiserver die Hardware- und Softwareanforderungen erfüllt, erstellen Sie zwei freigegebene Ordner für die Daten von Kaspersky Security Center und konfigurieren Sie die Berechtigungen für den Zugriff auf die freigegebenen Ordner.

   Anleitungen: Einen Dateiservers für das Kaspersky Failover Cluster vorbereiten

3. **Vorbereiten von aktiven und passiven Knoten**

   Bereiten Sie zwei Computer mit identischer Hardware und Software vor, um als aktive und passive Knoten zu fungieren.

   Anleitungen: Knoten für Kaspersky Failover Cluster vorbereiten

4. **Installieren des Datenbankmanagementsystems (DBMS)**

   Sie haben zwei Optionen:

   - Wenn Sie MariaDB Galera Cluster verwenden möchten, benötigen Sie keinen dedizierten Computer für das DBMS. Installieren Sie MariaDB Galera Cluster auf jedem der Knoten.
   - Wenn Sie ein anderes unterstütztes DBMS verwenden möchten, installieren Sie das ausgewählte DBMS auf einem dedizierten Computer.

5. **Installieren von Kaspersky Security Center**

   Installieren Sie Kaspersky Security Center im Modus für Failover-Cluster auf beiden Knoten. Sie müssen Kaspersky Security Center zunächst auf dem aktiven Knoten installieren und anschließend auf dem passiven.

6. **Testen des Failover-Clusters**

   Überprüfen Sie, ob Sie das Failover Cluster richtig konfiguriert haben und ob es ordnungsgemäß funktioniert. Sie können beispielsweise einen der Dienste von Kaspersky Security Center auf dem aktiven Knoten stoppen: kladminserver, klnagent, ksnproxy, klactprx oder klwebsrv. Wenn der Dienst angehalten wird, muss die Schutzverwaltung automatisch auf den passiven Knoten umschalten.

Ergebnisse

Das Kaspersky Failover Cluster wurde bereitgestellt. Bitte informieren Sie sich über die Ereignisse, die zum Umschalten zwischen dem aktiven und passiven Knoten führen.

Über das Kaspersky Failover Cluster

Ein Kaspersky-Failover-Cluster bietet eine hohe Verfügbarkeit für Kaspersky Security Center und minimiert die Ausfallzeit des Administrationsservers im Falle eines Fehlers. Das Failover-Cluster basiert auf zwei identischen Instanzen von Kaspersky Security Center, die auf zwei Computern installiert sind. Eine der Instanzen arbeitet als aktiver Knoten und die andere ist ein passiver Knoten. Der aktive Knoten verwaltet den Schutz der Client-Geräte, während der passive bereit ist, alle Funktionen des aktiven Knotens zu übernehmen, falls der aktive Knoten ausfällt. Wenn ein Fehler auftritt, wird der passive Knoten aktiv und der aktive Knoten wird passiv.

In einem Kaspersky Failover Cluster werden alle Kaspersky Security Center-Dienste automatisch verwaltet. Versuchen Sie nicht, die Dienste manuell neu zu starten.

Hard- und Softwarevoraussetzungen

Um ein Kaspersky-Failover-Cluster bereitzustellen, benötigen Sie die folgende Hardware:

- Zwei Computer mit identischer Hard- und Software. Diese Computer fungieren als aktive und passive Knoten.
- Ein Dateiserver unter Linux mit dem EXT4-Dateisystem. Sie müssen einen dedizierten Computer bereitstellen, der als Dateiserver fungiert.

  Stellen Sie sicher, dass Sie eine hohe Netzwerkbandbreite zwischen dem Dateiserver und den aktiven und passiven Knoten bereitgestellt haben.

- Ein Computer mit Datenbankverwaltungssystem (DBMS). Wenn Sie MariaDB Galera Cluster als DBMS verwenden, ist für diesen Zweck kein dedizierter Computer erforderlich.

Umschaltbedingungen

Das Failover Cluster schaltet die Verwaltung des Schutzes der Client-Geräte vom aktiven Knoten auf den passiven Knoten um, wenn auf dem aktiven Knoten eines der folgenden Ereignisse auftritt:

- Der aktive Knoten ist aufgrund eines Software- oder Hardwarefehlers defekt.
- Der aktive Knoten wurde für Wartungsaktivitäten vorübergehend gestoppt.
- Mindestens einer der Dienste (oder Prozesse) von Kaspersky Security Center ist fehlgeschlagen oder wurde vom Benutzer absichtlich beendet. Die Dienste von Kaspersky Security Center sind: kladminserver, klnagent, klactprx und klwebsrv.
- Die Netzwerkverbindung zwischen dem aktiven Knoten und dem Speicher auf dem Dateiserver wurde unterbrochen oder beendet.

Einen Dateiservers für ein Kaspersky-Failover-Cluster vorbereiten

Der Dateiserver ist eine erforderliche Komponente für das Kaspersky Failover-Cluster.

So bereiten Sie einen Dateiserver vor:

1. Stellen Sie sicher, dass der Dateiserver die Hardware- und Softwareanforderungen erfüllt.
2. Installieren und konfigurieren Sie einen NFS-Server:
   - Der Zugriff auf den Dateiserver muss für beide Knoten in den NFS-Servereinstellungen aktiviert werden.
   - Das NFS-Protokoll muss die Version 4.0 oder 4.1 haben.
   - Mindestanforderungen für den Linux-Kernel:
     - 3.19.0-25, wenn Sie NFS 4.0 verwenden
     - 4.4.0-176, wenn Sie NFS 4.1 verwenden
3. Erstellen Sie auf dem Dateiserver zwei Ordner und geben Sie sie mithilfe von NFS frei. Einer von ihnen wird verwendet, um Informationen über den Status des Failover-Clusters zu speichern. Der andere dient zum

Speichern der Daten und Einstellungen von Kaspersky Security Center. Während der Konfiguration der Installation von Kaspersky Security Center müssen Sie die Pfade zu den freigegebenen Ordnern angeben.

Führen Sie die folgenden Befehle aus:

```
sudo yum install nfs-utils
sudo mkdir -p /mnt/KlFocStateShare
sudo mkdir -p /mnt/KlFocDataShare_klfoc
sudo chown ksc:kladmins /mnt/KlFocStateShare
sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
sudo chmod -R 777 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >>
/etc/exports"
sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\
(rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
sudo cat /etc/exports
sudo exportfs -a
sudo systemctl start rpcbind
sudo service nfs start
```

Aktivieren Sie den Autostart, indem Sie den folgenden Befehl ausführen:

```
sudo systemctl enable rpcbind
```

4. Starten Sie den Dateiserver neu.

Der Dateiserver ist vorbereitet. Um das Kaspersky-Failover-Cluster bereitzustellen, folgen Sie den weiteren Anweisungen in diesem Szenario.

Die Knoten für ein Kaspersky-Failover-Cluster vorbereiten

Bereiten Sie zwei Computer darauf vor, als aktiver und passiver Knoten für das Kaspersky Failover Cluster zu fungieren.

Um die Knoten für das Kaspersky Failover Cluster vorzubereiten:

1. Stellen Sie sicher, dass Sie über zwei Computer verfügen, welche die Hardware- und Softwareanforderungen erfüllen. Diese Computer fungieren als aktive und passive Knoten des Failover-Clusters.

2. Damit die Knoten als NFS-Clients fungieren, installieren Sie auf beiden Knoten das Paket nfs-utils.

   führen Sie den folgenden Befehl aus:

   ```
   sudo yum install nfs-utils
   ```

3. Erstellen Sie Bereitstellungspunkte, indem Sie die folgenden Befehle ausführen:

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   ```

4. Überprüfen Sie, ob die freigegebenen Ordner erfolgreich bereitgestellt wurden. [optionaler Schritt]

   Führen Sie die folgenden Befehle aus:

   ```
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,auto,user,rw {server}:{path to
   the KlFocStateShare folder} /mnt/KlFocStateShare
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw {server}:{path to
   the KlFocDataShare_klfoc folder} /mnt/KlFocDataShare_klfoc
   ```

   Dabei sind `{server}:{path to the KlFocStateShare folder}` und `{server}:{path to the KlFocDataShare_klfoc folder}` die Netzwerkpfade der freigegebenen Ordner auf dem Dateiserver.

Nachdem die freigegebenen Ordner erfolgreich bereitgestellt wurden, heben Sie die Bereitstellung auf, indem Sie die folgenden Befehle ausführen:

```
sudo umount /mnt/KlFocStateShare
sudo umount /mnt/KlFocDataShare_klfoc
```

5. Passen Sie die Bereitstellungspunkte und die freigegebenen Ordner an:
   ```
   sudo vi /etc/fstab
   {server}:{path to the KlFocStateShare folder} /mnt/KlFocStateShare nfs
   vers=4,nolock,local_lock=none,auto,user,rw 0 0
   {server}:{path to the KlFocDataShare_klfoc folder} /mnt/KlFocDataShare_klfoc nfs
   vers=4,nolock,local_lock=none,noauto,user,rw 0 0
   ```
   Dabei sind `{server}:{path to the KlFocStateShare folder}` und `{server}:{path to the KlFocDataShare_klfoc folder}` die Netzwerkpfade der freigegebenen Ordner auf dem Dateiserver.

6. Starten Sie beide Knoten neu.

7. Stellen Sie die freigegebenen Ordner bereit, indem Sie die folgenden Befehle ausführen:
   ```
   mount /mnt/KlFocStateShare
   mount /mnt/KlFocDataShare_klfoc
   ```

8. Stellen Sie sicher, dass die Berechtigungen für den Zugriff auf die freigegebenen Ordner ksc:kladmins gehören.

   führen Sie den folgenden Befehl aus:

   ```
   sudo ls -la /mnt/
   ```

9. Führen Sie eine der folgenden Aktionen aus:

   - Erstellen Sie auf jedem der Knoten einen virtuellen Netzwerkadapter. Führen Sie beispielsweise die folgenden Befehle aus:

     a. Ermitteln Sie die Schnittstellennamen, indem Sie den folgenden Befehl ausführen:
     ```
     ifconfig
     ```

     b. Führen Sie das folgende Skript aus (die unten angegebenen Schnittstellennamen sind als Beispiele gedacht):
     ```
     #!/bin/bash
     PHYSICAL_IFACE=ens160
     VIRTUAL_IFACE=macvlan1
     ip link del $VIRTUAL_IFACE > /dev/null 2>&1
     ip link add link $PHYSICAL_IFACE $VIRTUAL_IFACE type macvlan
     if [ "$?" -ne "0" ]; then
         echo ERROR adding new virtual adapter $VIRTUAL_IFACE!
         exit $?
     fi
     ip link set $VIRTUAL_IFACE down
     if [ "$?" -ne "0" ]; then
         echo ERROR disabling virtual adapter $VIRTUAL_IFACE!
         exit $?
     fi
     ```

     c. Führen Sie den folgenden Befehl aus:
     ```
     ip addr add {IP-Adresse des virtuellen Netzwerkadapters} dev {Name des
     virtuellen Netzwerkadapters}
     ```

     Die IP-Adresse muss leer sein, wenn Sie den virtuellen Netzwerkadapter erstellen. Die virtuellen Netzwerkadapter müssen auf beiden Knoten dieselbe IP-Adresse haben.

     d. Überprüfen Sie, ob der virtuelle Netzwerkadapter erfolgreich erstellt wurde.

Führen Sie die folgenden Befehle aus:

```
ip link set macvlan1 up
ifconfig
```

e. Deaktivieren Sie den virtuellen Netzwerkadapter, indem Sie den folgenden Befehl ausführen:

```
ip link set macvlan1 down
```

- Verwenden Sie den Load Balancer eines Drittanbieters. Sie können beispielsweise einen nginx-Server verwenden. Gehen Sie in diesem Fall wie folgt vor:

  a. Stellen Sie einen dedizierten Linux-basierten Computer mit installiertem nginx bereit.

  b. Konfigurieren Sie das Load Balancing. Legen Sie den aktiven Knoten als Hauptserver und den passiven Knoten als Backup-Server fest.

  c. Öffnen Sie auf dem nginx-Server alle Ports des Administrationsservers: TCP 13000, UDP 13000, TCP 13291, TCP 13299, TCP 17000.

Die Knoten sind vorbereitet. Um das Kaspersky Failover Cluster bereitzustellen, folgen Sie den weiteren Anweisungen des Szenarios.

Kaspersky Security Center auf den Knoten des Kaspersky-Failover-Clusters installieren

Dieses Verfahren beschreibt die Installation von Kaspersky Security Center auf den Knoten des Kaspersky Failover Clusters. Kaspersky Security Center wird auf beiden Knoten des Kaspersky-Failover-Clusters separat installiert. Installieren Sie das Programm zunächst auf dem aktiven Knoten und anschließend auf dem passiven. Bei der Installation legen Sie fest, welcher Knoten als aktiv und welcher als passiv fungieren soll.

Verwenden Sie die Installationsdatei ksc64_[Versionsnummer]_amd64.deb oder ksc64-[Versionsnummer].x86_64.rpm, die der auf Ihrem Gerät installierten Linux-Distribution entspricht. Sie erhalten die Installationsdatei, indem Sie sie von der Kaspersky-Website herunterladen.

Nur ein Benutzer aus der Domänengruppe "KLAdmins" kann Kaspersky Security Center auf jedem Knoten installieren.

Installation auf dem primären (aktiven) Knoten

Um Kaspersky Security Center auf dem primären Knoten zu installieren:

1. Stellen Sie sicher, dass auf dem Gerät, auf dem Sie Kaspersky Security Center installieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.

2. Führen Sie in der Befehlszeile unter einem Benutzerkonto mit Root-Rechten die in dieser Anleitung genannten Befehle aus.

3. Führen Sie die Installation von Kaspersky Security Center aus. Führen Sie abhängig von Ihrer Linux-Distribution einen der folgenden Befehle aus:

   - `sudo apt install /<path>/ksc64_[Versionsnummer]_amd64.deb`

- `sudo yum install /<path>/ksc64-[Versionsnummer].x86_64.rpm -y`

4. Konfigurieren Sie Kaspersky Security Center:

   `sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`

5. Lesen Sie den Endbenutzer-Lizenzvertrag (EULA) und die Datenschutzrichtlinie. Der Text wird im Befehlszeilenfenster angezeigt. Drücken Sie die Leertaste, um das nächste Textsegment anzuzeigen. Geben Sie nach der entsprechenden Aufforderung die folgenden Werte ein:

   a. Geben Sie `y` ein, wenn Sie die EULA-Bedingungen verstehen und akzeptieren. Geben Sie `n` ein, wenn Sie den EULA-Bedingungen nicht zustimmen. Um Kaspersky Security Center zu nutzen, müssen Sie den Bestimmungen des Endbenutzer-Lizenzvertrags (EULA) zustimmen.

   b. Geben Sie `y` ein, wenn Sie die Bedingungen der Datenschutzrichtlinie verstehen und akzeptieren, und Sie damit einverstanden sind, dass Ihre Daten so verarbeitet und (einschließlich in Drittländer) übertragen werden, wie es in der Datenschutzrichtlinie beschrieben ist. Geben Sie `n` ein, wenn Sie den Bedingungen der Datenschutzrichtlinie nicht zustimmen. Um Kaspersky Security Center zu nutzen, müssen Sie den Bestimmungen der Datenschutzrichtlinie zustimmen.

6. Wählen Sie **Primärer Cluster-Knoten** als Installationsmodus des Administrationsservers aus.

7. Geben Sie nach der entsprechenden Aufforderung die folgenden Einstellungen ein:

   a. Geben Sie den lokalen Pfad des Bereitstellungspunkts des Status-Netzwerkordners ein.

   b. Geben Sie den lokalen Pfad zum Bereitstellungspunkt des Daten-Netzwerkordners ein.

   c. Wählen Sie einen Failover Cluster-Konnektivitätsmodus aus: über einen virtuellen Netzwerkadapter oder einen externen Load Balancer.

   d. Wenn Sie einen virtuellen Netzwerkadapter verwenden, geben Sie seinen Namen ein.

   e. Wenn Sie aufgefordert werden, den DNS-Namen oder die statische IP-Adresse des Administrationsservers einzugeben, geben Sie die IP-Adresse des virtuellen Netzwerkadapters oder die IP-Adresse des externen Load Balancers ein.

   f. Geben Sie die Portnummer des Administrationsservers ein. Standardmäßig ist die Portnummer 14000 festgelegt.

   g. Geben Sie die SSL-Portnummer des Administrationsservers ein. Standardmäßig ist die Portnummer 13000 festgelegt.

   h. Ermitteln Sie die ungefähre Anzahl der Geräte, die Sie verwalten möchten:

      - Geben Sie für 1 bis 100 vernetzte Geräte den Wert 1 ein.
      - Geben Sie für 101 bis 1.000 vernetzte Geräte den Wert 2 ein.
      - Geben Sie für über 1.000 vernetzte Geräte den Wert 3 ein.

   i. Geben Sie den Namen der Sicherheitsgruppe für Dienste ein. Standardmäßig wird die Gruppe 'kladmins' verwendet.

   j. Geben Sie den Namen des Benutzerkontos ein, um den Administrationsserver-Dienst zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein. Standardmäßig wird das Konto 'ksc' verwendet.

k. Geben Sie den Namen des Benutzerkontos ein, um andere Dienste zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein. Standardmäßig wird das Konto 'ksc' verwendet.

l. Geben Sie die IP-Adresse des Gerätes ein, auf dem die Datenbank installiert ist.

m. Geben Sie die Portnummer der Datenbank ein. Dieser Port wird für die Kommunikation mit dem Administrationsserver verwendet. Standardmäßig ist die Portnummer 3306 festgelegt.

n. Geben Sie den Namen der Datenbank ein.

o. Geben Sie den Benutzernamen des Datenbank-Root-Benutzerkontos ein, das Sie für den Zugriff auf die Datenbank verwenden.

p. Geben Sie das Kennwort des Datenbank-Root-Benutzerkontos ein, das Sie für den Zugriff auf die Datenbank verwenden.

Warten Sie, bis die Dienste hinzugefügt und automatisch gestartet wurden:

- klnagent_srv
- kladminserver_srv
- klactprx_srv
- klwebsrv_srv

q. Erstellen Sie ein Benutzerkonto, das als Administrator des Administrationsservers fungiert. Geben Sie den Benutzernamen und das Kennwort ein. Das Benutzerkennwort muss mindestens 8 Zeichen und darf maximal 16 Zeichen enthalten.

Der Benutzer wird hinzugefügt und Kaspersky Security Center wird auf dem primären Knoten installiert.

Installation auf dem sekundären (passiven) Knoten

Um Kaspersky Security Center auf dem sekundären Knoten zu installieren:

1. Stellen Sie sicher, dass auf dem Gerät, auf dem Sie Kaspersky Security Center installieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.
2. Führen Sie in der Befehlszeile unter einem Benutzerkonto mit Root-Rechten die in dieser Anleitung genannten Befehle aus.
3. Führen Sie die Installation von Kaspersky Security Center aus. Führen Sie abhängig von Ihrer Linux-Distribution einen der folgenden Befehle aus:
   - `sudo apt install /<path>/ksc64_[Versionsnummer]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[Versionsnummer].x86_64.rpm -y`
4. Konfigurieren Sie Kaspersky Security Center:

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Lesen Sie den Endbenutzer-Lizenzvertrag (EULA) und die Datenschutzrichtlinie. Der Text wird im Befehlszeilenfenster angezeigt. Drücken Sie die Leertaste, um das nächste Textsegment anzuzeigen. Geben Sie nach der entsprechenden Aufforderung die folgenden Werte ein:

a. Geben Sie `y` ein, wenn Sie die EULA-Bedingungen verstehen und akzeptieren. Geben Sie `n` ein, wenn Sie den EULA-Bedingungen nicht zustimmen. Um Kaspersky Security Center zu nutzen, müssen Sie den Bestimmungen des Endbenutzer-Lizenzvertrags (EULA) zustimmen.

b. Geben Sie `y` ein, wenn Sie die Bedingungen der Datenschutzrichtlinie verstehen und akzeptieren, und Sie damit einverstanden sind, dass Ihre Daten so verarbeitet und (einschließlich in Drittländer) übertragen werden, wie es in der Datenschutzrichtlinie beschrieben ist. Geben Sie `n` ein, wenn Sie den Bedingungen der Datenschutzrichtlinie nicht zustimmen. Um Kaspersky Security Center zu nutzen, müssen Sie den Bestimmungen der Datenschutzrichtlinie zustimmen.

6. Wählen Sie **Sekundärer Cluster-Knoten** als Installationsmodus des Administrationsservers aus.

7. Geben Sie bei Aufforderung den lokalen Pfad des Bereitstellungspunkts des Status-Netzwerkordners ein.

Kaspersky Security Center wird auf dem sekundären Knoten installiert.

Überprüfung von Diensten

Verwenden Sie die folgenden Befehle, um zu überprüfen, ob ein Dienst ausgeführt wird oder nicht:

- `systemctl status klnagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`
- `systemctl status klwebsrv_srv.service`

Sie können jetzt das Kaspersky-Failover-Cluster testen, um sicherzustellen, dass Sie es richtig konfiguriert haben und dass das Cluster ordnungsgemäß funktioniert.

Cluster-Knoten manuell starten und beenden

Möglicherweise müssen Sie das gesamten Kaspersky-Failover-Cluster stoppen oder einen der Cluster-Knoten zu Wartungszwecken vorübergehend trennen. Folgen Sie in diesem Fall den Anweisungen in diesem Abschnitt. Versuchen Sie nicht, die Dienste oder Prozesse im Zusammenhang mit dem Failover-Cluster auf eine andere Weise zu starten oder zu stoppen. Dies kann zu Datenverlust führen.

Starten und Stoppen des gesamten Failover-Clusters zu Wartungszwecken

So starten oder stoppen Sie das gesamten Failover-Cluster:

1. Gehen Sie im aktiven Knoten zu /opt/kaspersky/ksc64/sbin.

2. Öffnen Sie die Befehlszeile und führen Sie einen der folgenden Befehle aus:

   - Um das Cluster zu stoppen: `klfoc -stopcluster --stp klfoc`
   - Um das Cluster zu starten: `klfoc -startcluster --stp klfoc`

Das Failover-Cluster wird je nach ausgeführtem Befehl gestartet oder gestoppt.

Wartung eines Knotens

So warten Sie einen der Knoten:

1. Stoppen Sie auf dem aktiven Knoten das Failover-Cluster mit dem Befehl `klfoc -stopcluster --stp klfoc`.
2. Gehen Sie im Knoten, den Sie verwalten möchten, zu /opt/kaspersky/ksc64/sbin.
3. Öffnen Sie die Befehlszeile und trennen Sie anschließend den Knoten vom Cluster, indem Sie den Befehl `detach_node.sh` ausführen.
4. Starten Sie auf dem aktiven Knoten das Failover-Cluster mit dem Befehl `klfoc -startcluster --stp klfoc`.
5. Führen Sie die Wartungsarbeiten durch.
6. Stoppen Sie auf dem aktiven Knoten das Failover-Cluster mit dem Befehl `klfoc -stopcluster --stp klfoc`.
7. Gehen Sie im verwalteten Knoten zu /opt/kaspersky/ksc64/sbin.
8. Öffnen Sie die Befehlszeile und fügen Sie den Knoten anschließend wieder an das Cluster an, indem Sie den Befehl `attach_node.sh` ausführen.
9. Starten Sie auf dem aktiven Knoten das Failover-Cluster mit dem Befehl `klfoc -startcluster --stp klfoc`.

Der Knoten ist gewartet und an das Failover-Cluster angehängt.

Zertifikate für die Ausführung mit Kaspersky Security Center

Dieser Abschnitt enthält Informationen über die Zertifikate für Kaspersky Security. Außerdem wird hier beschrieben, wie Sie Zertifikate für Kaspersky Security Center 14 Web Console ausstellen und ersetzen und wie Sie ein Zertifikat für den Administrationsserver erneuern, wenn der Server mit Kaspersky Security Center 14 Web Console interagiert.

Über die Zertifikate von Kaspersky Security Center

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

- Zertifikat des Administrationsservers
- Zertifikat des Webservers
- Zertifikat der Kaspersky Security Center 14 Web Console

Standardmäßig verwendet Kaspersky Security Center selbstsignierte Zertifikate (d.h., sie werden von Kaspersky Security Center selbst ausgestellt). Sie können diese jedoch durch benutzerdefinierte Zertifikate ersetzen, um den Sicherheitsanforderungen Ihres Unternehmensnetzwerks sowie Sicherheitsstandards besser zu entsprechen. Nachdem der Administrationsserver sichergestellt hat, dass das benutzerdefinierte Zertifikat alle notwendigen Anforderungen erfüllt, nimmt das Zertifikat den gleichen Funktionsumfang wie ein selbstsigniertes Zertifikat an. Der einzige Unterschied besteht darin, dass ein benutzerdefiniertes Zertifikat nach dessen Ablauf nicht automatisch neu ausgestellt wird. Zertifikate können durch benutzerdefinierte Zertifikate ersetzt werden, indem Sie entweder das Dienstprogramm klsetsrvcert verwenden oder je nach Zertifikattyp den Abschnitt "Eigenschaften des Administrationsservers" in Kaspersky Security Center 14 Web Console verwenden. Wenn Sie das Tool "klsetsrvcert" verwenden, müssen Sie für das Zertifikat einen Typ angeben, indem Sie einen der folgenden Werte verwenden:

- C – gewöhnliches Zertifikat für die Ports 13000 und 13291
- CR – gewöhnliches Reservezertifikat für die Ports 13000 und 13291

Zertifikate des Administrationsservers

Ein Zertifikat des Administrationsservers ist für folgende Zwecke erforderlich:

- Authentifizierung des Administrationsservers beim Verbinden mit Kaspersky Security Center 14 Web Console
- Sichere Interaktion zwischen dem Administrationsserver und dem Administrationsagenten auf verwalteten Geräten
- Authentifizierung, wenn die primären Administrationsserver mit sekundären Administrationsservern verbunden sind

Das Zertifikat des Administrationsservers wird bei der Installation der Komponente "Administrationsserver" automatisch erstellt und im Ordner /var/opt/kaspersky/klnagent_srv/1093/cert/ gespeichert. Das Zertifikat des Administrationsservers geben Sie an, wenn Sie eine Antwortdatei erstellen, um Kaspersky Security Center 14 Web Console zu installieren. Dieses Zertifikat wird als gewöhnliches Zertifikat (common - "C") bezeichnet.

Das Zertifikat des Administrationsservers ist für 397 Tage gültig. Kaspersky Security Center generiert CR-Zertifikat ("common reserve") automatisch 90 Tage vor Ablauf des gewöhnlichen Zertifikats. Das gewöhnliche Reservezertifikat wird daraufhin für das nahtlose Ersetzen des Zertifikats des Administrationsservers verwendet. Wenn das gewöhnliche Zertifikat im Begriff ist abzulaufen, wird das gewöhnliche Reservezertifikat verwendet, um die Verbindung mit den Instanzen der Administrationsagenten auf den verwalteten Geräten aufrecht zu erhalten. Aus diesem Grund wird 24 Stunden vor Ablauf des alten gewöhnlichen Zertifikates das gewöhnliche Reservezertifikat automatisch zum neuen gewöhnlichen Zertifikat.

> Wenn Sie mehr als 397 Tage für den Gültigkeitszeitraum des Administrationsserver-Zertifikats angeben, gibt der Web-Browser einen Fehler aus.

Bei Bedarf können Sie dem Administrationsserver ein benutzerdefiniertes Zertifikat zuweisen. Dies kann beispielsweise für eine bessere Integration in die vorhandene PKI Ihres Unternehmens oder für die benutzerdefinierte Konfiguration der Zertifikatfelder erforderlich sein. Beim Ersetzen des Zertifikates stellen alle Administrationsagenten, die zuvor mittels SSL mit Administrationsserver verbunden waren, keine Verbindung mit dem Server mehr her und geben den Fehler "Fehler bei der Authentifizierung des Administrationsservers" zurück. Um diesen Fehler zu beheben, müssen Sie die Verbindung nach dem Ersetzen des Zertifikats wiederherstellen.

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

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

Zertifikat des Webservers

Die Webserver-Komponente des Kaspersky Security Center Administrationsservers verwendet eine spezielle Art von Zertifikat. Dieses Zertifikat ist für die Veröffentlichung von Administrationsagenten-Installationspaketen erforderlich, die Sie anschließend auf verwaltete Geräte herunterladen. Aus diesem Grund kann der Webserver verschiedene Zertifikate verwenden.

Der Webserver verwendet eines der folgenden Zertifikate in der Reihenfolge ihrer Priorität:

1. Benutzerdefiniertes Zertifikat des Webservers, das Sie manuell in der Kaspersky Security Center 14 Web Console angegeben haben

2. Gewöhnliches Zertifikate des Administrationsservers ("C")

Zertifikat der Kaspersky Security Center 14 Web Console

Der Server von Kaspersky Security Center 14 Web Console (im Folgenden als Web Console bezeichnet) verfügt über ein eigenes Zertifikat. Wenn Sie eine Website öffnen, überprüft ein Browser, ob Ihre Verbindung vertrauenswürdig ist. Das Zertifikat der Web Console ermöglicht Ihnen die Authentifizierung der Web Console und wird verwendet, um den Datenverkehr zwischen einem Browser und der Web Console zu verschlüsseln.

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

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

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

Anforderungen an benutzerdefinierte Zertifikate für deren Verwendung in Kaspersky Security Center

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

Voraussetzungen für Zertifikate von Kaspersky Security Center

Typ des Zertifikats	Voraussetzungen	Kommentare
Gewöhnliches Zertifikat, gewöhnliches	Minimale Schlüssellänge: 2048 Basic constraints: • CA: true	Der Parameter für Extended Key Usage ist optional.

Reservezertifikat ("C", "CR")	• Path Length Constraint: None Schlüsselverwendung: • Digital signature • Certificate signing • Key encipherment • CRL Signing Extended Key Usage (optional): Serverauthentifizierung, Clientauthentifizierung	Der Wert von Path Length Constraint kann eine von "None" abweichende Integer-Zahl sein, aber darf nicht kleiner als "1" sein.
Zertifikat des Webservers	Extended Key Usage: Serverauthentifizierung Der PKCS #12- / PEM-Container, aus dem das Zertifikat angegeben wird, enthält die vollständige Kette der öffentlichen Schlüssel. Der "Subject Alternative Name" (SAN) des Zertifikats ist vorhanden. Das heißt, dass der Wert des Feldes `subjectAltName` zulässig ist. Das Zertifikat erfüllt die aktuell wirksamen Anforderungen des Webbrowsers an Serverzertifikate, sowie die aktuell gültigen Grundvoraussetzungen des CA/Browser Forums.	Nicht anwendbar.
Zertifikat der Kaspersky Security Center 14 Web Console	Der PEM-Container, aus dem das Zertifikat angegeben wird, enthält die vollständige Kette der öffentlichen Schlüssel. Der "Subject Alternative Name" (SAN) des Zertifikats ist vorhanden. Das heißt, dass der Wert des Feldes `subjectAltName` zulässig ist. Das Zertifikat erfüllt die aktuell wirksamen Anforderungen des Webbrowsers an Serverzertifikate, sowie die aktuell gültigen Grundvoraussetzungen des CA/Browser Forums.	Verschlüsselte Zertifikate werden von Kaspersky Security Center 14 Web Console nicht unterstützt.

Zertifikat für Kaspersky Security Center 14 Web Console erneut ausstellen

Die meisten Browser legen dem Zeitraum für die Gültigkeit eines Zertifikats ein Obergrenze auf. Um innerhalb dieser Begrenzung zu bleiben ist der Gültigkeitszeitraum des Zertifikats von Kaspersky Security Center 14 Web Console auf 397 Tage begrenzt. Sie können ein existierendes Zertifikat ersetzen, das von einer Zertifizierungsstelle (Certification Authority, CA) stammt. Dazu stellen Sie ein neues selbstsigniertes Zertifikat aus. Als Alternative können Sie Ihr abgelaufenes Zertifikat für Kaspersky Security Center 14 Web Console erneut ausstellen.

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

- Geben Sie bei der Neuausstellung des Zertifikats ein benutzerdefiniertes Zertifikat an (empfohlene Option). Erstellen Sie ein Zertifikat, das in Ihrer Infrastruktur vertrauenswürdig ist und das die Anforderungen an benutzerdefinierte Zertifikate erfüllt.

- Fügen Sie das Zertifikat der Web Console nach der Neuausstellung der Liste mit vertrauenswürdigen Browser-Zertifikaten hinzu. Es wird empfohlen, dass Sie diese Option nur verwenden, wenn Sie kein benutzerdefiniertes Zertifikat erstellen können.

Um ein abgelaufenes Zertifikat für Kaspersky Security Center 14 Web Console erneut auszustellen:

Installieren Sie Kaspersky Security Center 14 Web Console neu. Dafür gibt es die folgenden Methoden:

- Wenn Sie dieselbe Installationsdatei für Kaspersky Security Center 14 Web Console verwenden möchten, entfernen Sie Kaspersky Security Center 14 Web Console und installieren Sie anschließend die gleiche Version von Kaspersky Security Center 14 Web Console.
- Wenn Sie eine Installationsdatei einer aktualisierten Version verwenden möchten, führen Sie den Upgrade-Befehl aus.

Das Zertifikat von Kaspersky Security Center 14 Web Console wurde erneut für einen weiteren Gültigkeitszeitraum von 397 Tagen ausgestellt.

Zertifikat für Kaspersky Security Center 14 Web Console ersetzen

Wenn Sie den Kaspersky Security Center 14 Web Console Server (auch Kaspersky Security Center 14 Web Console genannt) installieren, wird standardmäßig automatisch ein Browser-Zertifikat für das Programm generiert. Sie können das automatisch generierte Zertifikat mit einem eigenen ersetzen.

Um das Zertifikat für Kaspersky Security Center 14 Web Console mit einem eigenen zu ersetzen, gehen Sie wie folgt vor:

1. Erstellen Sie eine neue Antwortdatei, die für die Installation von Kaspersky Security Center 14 Web Console erforderlich ist.
2. Geben Sie in dieser Datei die Pfade der benutzerdefinierten Zertifikatsdatei und der Schlüsseldatei an. Verwenden Sie dazu den Parameter `certPath` und den Parameter `keyPath`.
3. Installieren Sie Kaspersky Security Center 14 Web Console neu, indem Sie die neue Antwortdatei angeben. Führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie dieselbe Installationsdatei für Kaspersky Security Center 14 Web Console verwenden möchten, entfernen Sie Kaspersky Security Center 14 Web Console und installieren Sie anschließend die gleiche Version von Kaspersky Security Center 14 Web Console.
   - Wenn Sie eine Installationsdatei einer aktualisierten Version verwenden möchten, führen Sie den Upgrade-Befehl aus.

Die Kaspersky Security Center 14 Web Console verwendet jetzt das angegebene Zertifikat.

Konvertieren eines pfx-Zertifikats in ein pem-Zertifikat

Um in Kaspersky Security Center 14 Web Console ein pfx-Zertifikat zu verwenden, müssen Sie dieses zunächst unter Verwendung eines beliebigen OpenSSL-basierten Cross-Plattform-Tools in ein pem-Format konvertieren.

So konvertieren Sie unter Linux ein pfx-Zertifikat in ein pem-Format:

1. Führen Sie in einem OpenSSL-basierten Cross-Plattform-Tool die folgenden Befehle aus:

   ```
   openssl pkcs12 -in <Dateiname.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > Server.crt
   ```

   ```
   openssl pkcs12 -in <Dateiname.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > Schlüssel.pem
   ```

2. Stellen Sie sicher, dass die Zertifikatsdatei und der private Schlüssel in dem gleichen Verzeichnis generiert werden, in dem sich die pfx-Datei befindet.

3. Kaspersky Security Center 14 Web Console unterstützt keine kennwortgeschützten Zertifikate. Führen Sie daher in einem OpenSSL-basierten, plattformübergreifenden Tool den folgenden Befehl aus, um das Kennwort von der pem-Datei zu entfernen:

   ```
   openssl rsa -in Schlüssel.pem -out Schlüssel-ohne-Kennwort.pem
   ```

   > Verwenden Sie für die Input- und Output-Dateien nicht denselben Namen.

   Daraufhin ist die neue pem-Datei nicht mehr kennwortgeschützt. Um sie zu verwenden, muss kein Kennwort mehr eingegeben werden.

Die crt- und die pem-Datei sind bereit zur Verwendung. Sie können diese im Installer von Kaspersky Security Center 14 Web Console angeben.

Szenario: Angeben des benutzerdefinierten Zertifikats des Administrationsservers

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

> Wenn Sie mehr als 397 Tage für den Gültigkeitszeitraum des Administrationsserver-Zertifikats angeben, gibt der Web-Browser einen Fehler aus.

Erforderliche Maßnahmen

Das neue Zertifikat muss im PKCS#12-Format erstellt werden (z. B. mittels PKI der Organisation) und von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt werden. Außerdem muss das neue Zertifikat die gesamte Vertrauenskette und einen privaten Schlüssel enthalten, welcher in der Datei mit der pfx- oder p12-Erweiterung gespeichert werden muss. Für das neue Zertifikat müssen unten aufgeführten Voraussetzungen erfüllt sein.

Zertifikatstyp: Gewöhnliches Zertifikat, gewöhnliches Reservezertifikat ("C", "CR")

Voraussetzungen:

- Minimale Schlüssellänge: 2048
- Basic constraints:
  - CA: true

- Path Length Constraint: None

  Der Wert von "Path Length Constraint" (Einschränkung der Pfadlänge) kann eine von "None" abweichende ganze Zahl sein, darf aber nicht kleiner als 1 sein.

- Schlüsselverwendung:
  - Digital signature
  - Certificate signing
  - Key encipherment
  - CRL Signing
- Extended Key Usage (EKU): Serverauthentifizierung und Clientauthentifizierung. Die EKU ist optional, aber wenn Ihr Zertifikat diese enthält, müssen die Authentifizierungsdaten für Server und Client in der EKU angegeben werden.

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

Schritte

Das Angeben des Zertifikats des Administrationsservers erfolgt schrittweise:

1. **Ersetzen des Zertifikat des Administrationsservers**

   Verwenden Sie dafür das Befehlszeilendienstprogramm klsetsrvcert.

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

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

Ergebnisse

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

Zertifikats des Administrationsservers mittels Dienstprogramm klsetsrvcert ersetzen

So ersetzen Sie das Zertifikat des Administrationsservers:

Führen Sie aus der Befehlszeile das folgenden Dienstprogramm aus:

```
klsetsrvcert [-t <Typ> {-i <Eingabedatei> [-p <Kennwort>] [-o <chkopt>] | -g <DNS-Name>}][-f <Zeit>][-r <calistfile>][-l <Protokolldatei>]
```

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

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

Parameterwerte des Dienstprogramms klsetsrvcert

Parameter	Wert
`-t <Typ>`	Typ des Zertifikats, das ersetzt werden muss. Mögliche Einstellungswerte des Parameters `<Typ>`: • `C` – gewöhnliches Zertifikat für die Ports 13000 und 13291 ersetzen. • `CR` – gewöhnliches Reservezertifikat für die Ports 13000 und 13291 ersetzen.
`-f <Zeit>`	Zeitplan für das Ersetzen der Zertifikate im Format "DD-MM-YYYY hh:mm" (für die Ports 13000 und 13291). Verwenden Sie diesen Parameter, wenn Sie das gewöhnliche Zertifikat oder das gewöhnliche Reservezertifikat ersetzen möchten, bevor es abläuft. Geben Sie die Zeit an, zu der verwaltete Geräte mit dem Administrationsserver mit einem neuen Zertifikat synchronisiert werden müssen.
`-I <Eingabedatei>`	Container mit dem Zertifikat und privatem Schlüssel im Format PKCS#12 (Datei mit der p12- oder pfx-Erweiterung).
`-p <Kennwort>`	Kennwort, mithilfe dessen der p12-Container geschützt ist. Da das Zertifikat und ein privater Schlüssel im Container gespeichert werden, wird das Kennwort benötigt, um die Datei mit dem Container zu entschlüsseln.
`-o <chkopt>`	Parameter der Zertifikatsvalidierung (durch Strichpunkt getrennt). Um ein benutzerdefiniertes Zertifikat ohne Signaturberechtigung zu verwenden, geben Sie im Dienstprogramm klsetsrvcert `-o NoCA` an. Dies ist nützlich für Zertifikate, die von einer öffentlichen Zertifizierungsstelle ausgestellt wurden.
`-g <DNS-Name>`	Ein neues Zertifikat wird für den angegebenen DNS-Namen erstellt.
`-r <calistfile>`	Liste mit vertrauenswürdigen Zertifizierungsstellen für Stammzertifikate im Format PEM.
`-l <Protokolldatei>`	Datei zur Ausgabe der Ergebnisse. Standardmäßig erfolgt die Ausgabe im Standardausgabestream.

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

```
klsetsrvcert -t C -i <Eingabedatei> -p <Kennwort> -o NoCA
```

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

Administrationsagenten mit dem Administrationsserver mittels Dienstprogramm klmover verbinden

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

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

Führen Sie aus der Befehlszeile das folgenden Dienstprogramm aus:

```
klmover [-address <Serveradresse>] [-pn <Portnummer>] [-ps <SSL-Portnummer>] [-nossl]
[-cert <Pfad zur Zertifikatsdatei>]
```

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

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

Parameterwerte des Dienstprogramms klmover

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

Angabe des freigegebenen Ordners

Nach der Installation des Administrationsservers können Sie den Speicherort des freigegebenen Ordners in den Eigenschaften des Administrationsservers angeben. Standardmäßig wird der freigegebene Ordner auf dem Gerät mit dem Administrationsserver erstellt. In einigen Fällen (wie hohe Belastung oder die Notwendigkeit des Zugriffes aus einem isolierten Netzwerk) ist es jedoch zweckmäßig, den freigegebenen Ordner auf einer speziellen Dateiressource zu erstellen.

Der freigegebene Ordner wird in einigen Szenarien der Softwareverteilung des Administrationsagenten verwendet.

Die Unterscheidung von Groß- und Kleinschreibung muss deaktiviert sein.

Über das Upgrade von Kaspersky Security Center Linux

Sie können Version 14 des Administrationsservers auf einem Gerät installieren, auf dem eine ältere Version des Administrationsservers installiert ist (ab Version 13). Beim Aktualisieren auf die Version 14 bleiben alle Daten und Einstellungen der vorherigen Version des Administrationsservers erhalten.

Während des Upgrades ist unbedingt darauf zu achten, dass keine gemeinsame Nutzung des DBMS durch den Administrationsserver und einer anderen Anwendung stattfindet.

Für das Upgrade einer Version des Administrationsservers gibt es die folgenden Methoden:

- Verwendung der Installationsdatei für Kaspersky Security Center
- Erstellen eines Backups der Administrationsserver-Daten, Installation einer neuen Version des Administrationsservers und Wiederherstellung der Administrationsserver-Daten aus dem Backup

Wenn Ihr Netzwerk mehrere Administrationsserver umfasst, müssen Sie jeden Server manuell aktualisieren. Ein zentralisiertes Upgrade wird von Kaspersky Security Center Linux nicht unterstützt.

Wenn Sie das Upgrade von Kaspersky Security Center Linux von einer älteren Version durchführen, werden alle installierten Plug-ins für unterstützte Kaspersky-Anwendungen beibehalten. Das Administrationsserver-Plug-in und Plug-in des Administrationsagenten werden automatisch aktualisiert.

Upgrade von Kaspersky Security Center Linux über die Installationsdatei

Um den Administrationsserver von einer früheren Version (ab Version 13) auf Version 14 upzugraden, können Sie mithilfe der Installationsdatei von Kaspersky Security Center eine neue Version über eine frühere Version installieren.

Um den Administrationsserver von einer älteren Version auf die Version 14 upzugraden:

1. Laden Sie die Installationsdatei für Kaspersky Security Center mit einem vollständigen Paket für Version 14 von der Kaspersky-Website herunter:
   - Für Geräte mit einem RPM-basierten Betriebssystem – ksc64-<Versionsnummer>-11247.x86_64.rpm
   - Für Geräte mit einem Debian-basierten Betriebssystem – ksc64_<Versionsnummer>-11247_amd64.deb
2. Upgraden Sie das Installationspaket mithilfe eines Paketmanagers, den Sie auf Ihrem Administrationsserver verwenden. Sie können beispielsweise die folgenden Befehle im Befehlszeilenterminal unter einem Benutzerkonto mit Root-Rechten verwenden:
   - Für Geräte mit einem RPM-basiertem Betriebssystem:
     ```
     $ sudo rpm -Uvh --nodeps --force ksc64-<Versionsnummer>-11247.x86_64.rpm
     ```
   - Für Geräte mit einem Debian-basiertem Betriebssystem:
     ```
     $ sudo dpkg -i ksc64_<Versionsnummer>-11247_amd64.deb
     ```

   Nachdem der Befehl erfolgreich ausgeführt wurde, wird das Skript /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl erstellt. Eine entsprechende Meldung wird im Terminal angezeigt.

3. Führen Sie das Skript /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl aus, um den aktualisierten Administrationsserver zu konfigurieren.

4. Lesen Sie den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie, die im Befehlszeilenterminal angezeigt werden. Wenn Sie mit allen Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind:

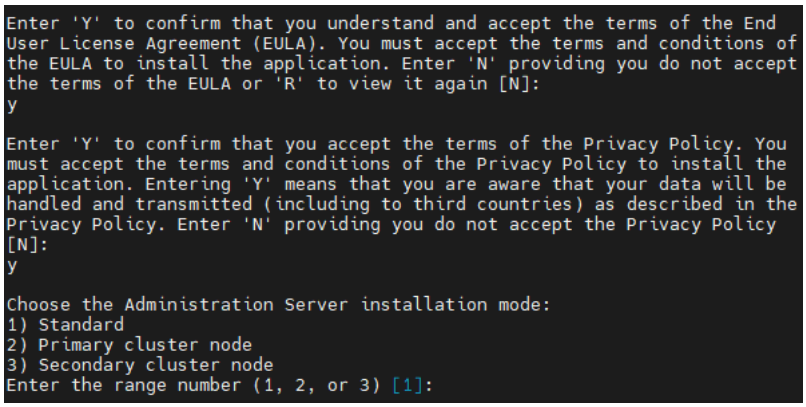
   a. Geben Sie "Y" ein, um zu bestätigen, dass Sie die Bedingungen des Endbenutzer-Lizenzvertrags vollständig gelesen und verstanden haben, und sie akzeptieren.

   b. Geben Sie erneut "Y" ein, um zu bestätigen, dass Sie die Datenschutzrichtlinie, die die Verarbeitung von Daten beschreibt, vollständig gelesen und verstanden haben, und sie akzeptieren.

   Nachdem Sie zwei Mal "Y" eingegeben haben, wird die Programminstallation auf Ihrem Gerät fortgesetzt.

5. Geben Sie "1" ein, um den Standard-Installationsmodus für den Administrationsserver auszuwählen.

   Das folgende Bild zeigt die letzten beiden Schritte.



Akzeptieren der Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie und Auswahl des Standard-Installationsmodus für den Administrationsserver im Befehlszeilenterminal

   Anschließend wird das Administrationsserver-Upgrade vom Skript konfiguriert und abgeschlossen. Während des Upgrades können Sie die vor dem Upgrade geänderten Einstellungen des Administrationsservers nicht ändern.

6. Für die Geräte, auf denen bereits die frühere Version des Administrationsagenten installiert ist, erstellen und starten Sie die Aufgabe zur Remote-Installation der neuen Version des Administrationsagenten.

   > Es wird empfohlen, den Administrationsagenten für Linux auf dieselbe Version zu aktualisieren, wie Kaspersky Security Center Linux.

   Nach Abschluss der Aufgabe zur Remote-Installation ist die Version des Administrationsagenten aktuell.

Upgrade von Kaspersky Security Center Linux über ein Backup

Um den Administrationsserver von einer früheren Version (ab Version 13) auf Version 14 upzugraden, können Sie ein Backup der Administrationsserver-Daten erstellen und diese Daten nach der Installation einer neuen Version von Kaspersky Security Center wiederherstellen. Sollten bei der Installation Probleme auftreten, können Sie die vorherige Version des Administrationsservers wiederherstellen, indem Sie die vor dem Update erstellte Backup-Kopie der Administrationsserver-Daten heranziehen.

Um den Administrationsserver über ein Backup von einer älteren Version auf die Version 14 upzugraden:

1. Erstellen Sie vor dem Upgrade ein Backup der Administrationsserver-Daten mit einer älteren Programmversion.
2. Deinstallieren Sie die ältere Version von Kaspersky Security Center.
3. Installieren Sie Kaspersky Security Center Version 14 auf dem bisherigen Administrationsserver.
4. Stellen Sie die Daten des Administrationsservers aus dem Backup, das vor dem Upgrade erstellt wurde, wieder her.
5. Für die Geräte, auf denen bereits die frühere Version des Administrationsagenten installiert ist, erstellen und starten Sie die Aufgabe zur Remote-Installation der neuen Version des Administrationsagenten.

   Es wird empfohlen, den Administrationsagenten für Linux auf dieselbe Version zu aktualisieren, wie Kaspersky Security Center Linux.

   Nach Abschluss der Aufgabe zur Remote-Installation ist die Version des Administrationsagenten aktuell.

In der Kaspersky Security Center 14 Web Console anmelden und abmelden

Sie können sich in der Kaspersky Security Center 14 Web Console anmelden, nachdem Sie den Administrationsserver und den Server der Web Console installiert haben. Sie müssen die während der Installation angegebene Webadresse des Administrationsservers und den Port kennen (der Standard-Port ist 8080). In Ihrem Browser muss JavaScript aktiviert sein.

Um sich in der Kaspersky Security Center 14 Web Console anzumelden, gehen Sie wie folgt vor:

1. Rufen Sie in Ihrem Browser <Webadresse des Administrationsservers>:<Port> auf.

   Die Anmeldeseite wird angezeigt.

2. Wenn Sie mehrere vertrauenswürdige Server hinzugefügt haben, wählen Sie in der Liste mit Administrationsservern den Administrationsserver aus, zu dem Sie eine Verbindung herstellen möchten.

   Wenn Sie nur einen einzigen Administrationsserver hinzugefügt haben, werden nur die Eingabefelder für Anmeldename und Kennwort angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:

   - Um sich an einem physischen Administrationsserver anzumelden, geben Sie den Benutzernamen und das Kennwort des lokalen Administrators ein.
   - Wenn auf dem Server mindestens ein virtueller Administrationsserver erstellt wurde und Sie sich an einem virtuellen Server anmelden möchten:

     a. Klicken Sie auf die Schaltfläche **Erweiterte Einstellungen**.

     b. Geben Sie den Namen des virtuellen Administrationsservers ein, den Sie während der Erstellung des virtuellen Servers angegeben haben.

     c. Geben Sie den Benutzernamen und das Passwort des Administrators ein, der die Berechtigungen für den virtuellen Administrationsserver besitzt.

Nach der Anmeldung wird das Dashboard in der Sprache und dem Design angezeigt, das Sie zuletzt verwendet haben. Sie können in der Kaspersky Security Center 14 Web Console navigieren und sie bei Ihrer Arbeit mit Kaspersky Security Center Linux nutzen.

Um die laufende Sitzung von Kaspersky Security Center 14 Web Console zu schließen, gehen Sie wie folgt vor:

1. Klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke des Bildschirms.
2. Wählen Sie im Dropdown-Menü den Punkt **Abmelden** aus.

Kaspersky Security Center 14 Web Console wird beendet und die Anmeldeseite wird angezeigt.

Schnellstartassistent

Mit Kaspersky Security Center Linux können Sie eine minimale Auswahl von Einstellungen anpassen, die für den Aufbau eines zentralisierten Verwaltungssystems für den Schutz Ihres Netzwerks vor Bedrohungen erforderlich sind. Diese Konfiguration wird mithilfe des Schnellstartassistenten für das Programm durchgeführt. Während der Ausführung des Assistenten können Sie die folgenden Änderungen a, Programm vornehmen:

- Schlüsseldateien hinzufügen oder Aktivierungscodes eingeben, die automatisch auf die Geräte der Administrationsgruppen verteilt werden können.
- E-Mail-Versand von Benachrichtigungen über Ereignisse konfigurieren, die vom Administrationsserver und den verwalteten Programmen registriert werden. (Damit Benachrichtigungen erfolgreich zugestellt werden, muss auf dem Administrationsserver und auf allen Geräten der Windows Messenger Dienst gestartet werden.)
- Schutzrichtlinien für Arbeitsstationen und Server sowie Aufgaben zur Untersuchung auf Viren, Update-Download und Verschieben ins Backup für die oberste Hierarchieebene der verwalteten Geräte erstellen.

  Der Schnellstartassistent erstellt Richtlinien nur für die Programme, deren Ordner **VERWALTETE GERÄTE** noch keine Richtlinien enthält. Der Schnellstartassistent erstellt keine Aufgaben, deren Namen mit den Aufgabennamen übereinstimmen, die für die obere Hierarchieebene der verwalteten Geräte bereits erstellt wurden.

Das Programm schlägt automatisch vor, beim ersten Verbindungsaufbau zum Server nach der Installation des Administrationsservers den Schnellstartassistenten zu starten. Sie können der Schnellstartassistent auch jederzeit manuell starten.

So starten Sie den Schnellstartassistenten manuell:

1. Klicken Sie im Hauptfenster der Anwendung auf das Symbol **Einstellungen** (⚙) 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 ausführen**.

Der Assistent schlägt vor, die ursprünglichen Einstellungen des Administrationsservers zu generieren. Folgen Sie den Anweisungen des Assistenten. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

Schritt 1. Einstellungen der Internetverbindung angeben

Legen Sie die Einstellungen für den Internetzugang von Kaspersky Security Center Linux fest.

Aktivieren Sie das Kontrollkästchen **Proxyserver verwenden**, wenn Sie einen Proxyserver für die Internetverbindung verwenden wollen. Wenn das Kontrollkästchen aktiviert ist, sind die Eingabefelder der Einstellungen verfügbar. Passen Sie die folgenden Verbindungseinstellungen für den Proxyserver an:

- **Adresse**
- **Port**

- Proxyserver für lokale Adressen umgehen

  Bei der Verbindung mit den Geräten im lokalen Netzwerk wird kein Proxyserver verwendet.

- Authentifizierung am Proxyserver

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

  Die Eingabefelder sind verfügbar, wenn das Kontrollkästchen **Proxyserver benutzen** aktiviert ist.

- Benutzername (Das Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist)

  Benutzerkonto, unter dem die Verbindung zum Proxyserver hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

- Kennwort (Das Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist)

  Kennwort, das von dem Benutzer festgelegt wird, unter dessen Benutzerkonto die Proxyserver-Verbindung hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

  Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen** und halten Sie sie für die erforderliche Zeitspanne gedrückt.

Schritt 2. Methode für die Programmaktivierung auswählen

Wählen Sie eine der folgenden Varianten zur Aktivierung von Kaspersky Security Center Linux aus:

- Durch Eingabe Ihres Aktivierungscodes

  Der *Aktivierungscode* ist eine eindeutige Zeichenfolge aus 20 Buchstaben und Ziffern. Den Aktivierungscode geben Sie ein, um einen Schlüssel zur Aktivierung von Kaspersky Security Center Linux hinzuzufügen. Sie erhalten den Aktivierungscode an die E-Mail-Adresse, die Sie beim Kauf von Kaspersky Security Center angegeben haben.

  Zur Aktivierung des Programms mithilfe eines Aktivierungscodes ist ein Internetzugang erforderlich, um sich mit den Aktivierungsservern von Kaspersky zu verbinden.

  Wenn Sie diese Aktivierungsoption ausgewählt haben, können Sie die Option **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** aktivieren.

  Wenn diese Option aktiviert ist, wird der Lizenzschlüssel automatisch an die verwalteten Geräte verteilt.

  Wenn diese Option deaktiviert ist, können Sie den Lizenzschlüssel später im Abschnitt **VORGÄNGE → LIZENZVERWALTUNG → LIZENZEN FÜR KASPERSKY-SOFTWARE** des Hauptmenüs an die verwalteten Geräte bereitstellen.

- Schlüsseldatei angeben

Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung key, die Sie von Kaspersky erhalten. Die Schlüsseldatei dient dazu, einen Schlüssel für die Aktivierung des Programms hinzuzufügen.

Sie erhalten Ihre Schlüsseldatei an die E-Mail-Adresse, die Sie beim Kauf von Kaspersky Security Center angegeben haben.

Um das Programm mit einer Schlüsseldatei zu aktivieren, ist keine Verbindung mit den Aktivierungsservern von Kaspersky erforderlich.

Wenn Sie diese Aktivierungsoption ausgewählt haben, können Sie die Option **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** aktivieren.

Wenn diese Option aktiviert ist, wird der Lizenzschlüssel automatisch an die verwalteten Geräte verteilt.

Wenn diese Option deaktiviert ist, können Sie den Lizenzschlüssel später im Abschnitt **VORGÄNGE → LIZENZVERWALTUNG → LIZENZEN FÜR KASPERSKY-SOFTWARE** des Hauptmenüs an die verwalteten Geräte bereitstellen.

- Verschieben Sie die Aktivierung des Programms

Wenn Sie die verschobene Aktivierung des Programms ausgewählt haben, können Sie den Lizenzschlüssel später jederzeit hinzufügen, indem Sie **VORGÄNGE → LIZENZVERWALTUNG** auswählen.

Wenn Sie mit Kaspersky Security Center aus einem gebührenpflichtigen AMI oder mit einem nutzungsbasierten, monatlich verrechneten SKU arbeiten, können Sie keine Schlüsseldateien angeben oder Aktivierungscodes eingeben.

Schritt 3. Grundlegenden Netzwerkschutz konfigurieren

Sie können die Liste mit Richtlinien und Aufgaben, die erstellt werden, überprüfen.

Bevor Sie zum nächsten Schritt des Assistenten wechseln können, müssen Sie warten, bis die Erstellung der Richtlinien und Aufgaben abgeschlossen ist.

Schritt 4. Einstellungen für das Senden von Benachrichtigungen

Passen Sie die Einstellungen für den Versand von Benachrichtigungen über Ereignisse an, die bei der Ausführung von Kaspersky-Programmen auf den Client-Geräten registriert werden. Diese Einstellungen werden in den Richtlinien für die Anwendungen als Standardwerte verwendet.

Folgende Einstellungen für den Versand von Benachrichtigungen über auftretende Ereignisse der Programme von Kaspersky können angepasst werden:

- Empfänger (E-Mail-Adressen)

  E-Mail-Adressen des Nutzers, an die das Programm Benachrichtigungen versenden soll. Sie können eine oder mehrere Adressen angeben. Geben Sie mehrere Adressen durch Semikolon getrennt an.

- SMTP-Serveradresse

Adresse oder Adressen der Mail-Server Ihres Unternehmens.

Geben Sie mehrere Adressen durch Semikolon getrennt an. Sie können folgende Parameterwerte verwenden:

- IPv4- oder IPv6-Adresse
- DNS-Name des SMTP-Servers

- **Port des SMTP-Servers**

  Kommunikationsportnummer des SMTP-Servers Standardmäßig ist Portnummer 25 angegeben.

- **ESMTP-Authentifizierung verwenden**

  Aktivierung der Unterstützung von ESMTP-Authentifizierung. Nach der Aktivierung des Kontrollkästchens in den Feldern **Benutzername** und **Kennwort** können die Einstellungen für ESMTP-Authentifizierung angeben werden. In der Standardeinstellung ist das Kontrollkästchen deaktiviert, und die Einstellungen der ESMTP-Authentifizierung sind nicht verfügbar.

Sie können die festgelegten Versandeinstellungen der E-Mail-Benachrichtigungen mithilfe der Schaltfläche **Testnachricht senden** prüfen.

Schritt 5. Schnellstartassistent abschließen

Klicken Sie auf **Fertigstellen**, um den Assistenten zu schließen.

Nachdem Sie den Schnellstartassistenten abgeschlossen haben, können Sie den Assistenten für die Bereitstellung des Schutzes ausführen um Schutzprogramme oder den Administrationsagenten automatisch auf Geräten in Ihrem Netzwerk zu installieren.

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 von 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**.

Wenn Sie den Administrationsagenten auf Geräten mit dem Betriebssystem SUSE Linux Enterprise Server 15 installieren möchten, sollten Sie zunächst das Paket insserv-compat installieren, um den Administrationsagenten konfigurieren.

Assistent für die Bereitstellung des Schutzes starten

Sie können den Assistenten für die Bereitstellung des Schutzes jederzeit manuell starten.

Um den Assistenten für die Bereitstellung des Schutzes manuell zu starten, gehen Sie wie folgt vor:

Klicken Sie im Hauptfenster des Programms auf **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. Installationspaket auswählen

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. Methode zur Verteilung einer Schlüsseldatei oder eines Aktivierungscodes auswählen

Wählen Sie eine Methode zur Verteilung einer Schlüsseldatei oder eines Aktivierungscodes aus:

- **Lizenzschlüssel nicht zum Installationspaket hinzufügen**

  Der Schlüssel wird automatisch auf alle Geräte verteilt, mit denen er kompatibel ist:

  - Wenn in den Eigenschaften des Schlüssel die automatische Verteilung aktiviert ist.
  - Wenn die Aufgabe **Schlüssel hinzufügen** erstellt wurde.

- **Lizenzschlüssel zum Installationspaket hinzufügen**

  Der Schlüssel wird gemeinsam mit dem Installationspaket verteilt.

  Es wird nicht empfohlen, den Schlüssel auf diese Art zu verteilen, da die Datenverwaltung der Installationspakete über allgemeinen Lesezugriff verfügt.

Wenn eine Schlüsseldatei oder ein Aktivierungscode bereits zum Installationspaket gehören, wird dieses Fenster angezeigt; enthält dann aber nur Informationen über den Lizenzschlüssel.

Schritt 3. Version des Administrationsagenten auswählen

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 4. Geräte auswählen

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 5. Einstellungen für die Aufgabe Remote-Installation festlegen

Passen Sie auf der Seite **Einstellungen für die Aufgabe zur Remote-Installation** die Einstellungen für die Remote-Installation eines Programms.

Wählen Sie in der Einstellungsgruppe **Download des Installationspakets erzwingen** die Methode der Übertragung der zur Programminstallation erforderlichen Dateien auf die Client-Geräte aus:

- **Unter Nutzung des Administrationsagenten**

  Wenn die Option aktiviert ist, werden die Installationspakete von dem auf den Client-Geräten installierten Administrationsagenten zugestellt.

  Wenn diese Option deaktiviert ist, werden Installationspakete über Tools des Linux-Betriebssystems 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 6. Inkompatible Programme vor der Installation deinstallieren

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 Linux 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. Geräte in "Verwaltete Geräte" verschieben

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 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. Benutzerkonten für den Zugriff auf Geräte auswählen

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)**

  Wenn diese Variante ausgewählt ist, kann das Konto angegeben werden, unter dem das Installationsprogramm gestartet werden soll. Das Benutzerkonto kann für den Fall angegeben werden, dass der Administrationsagent auf den Geräten, für die diese Aufgabe vorgesehen ist, nicht installiert ist.

  Sie können mehrere Benutzerkonten angeben, wenn beispielsweise kein Konto 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.

  Wenn kein Benutzerkonto hinzugefügt wurde, wird die Aufgabe unter dem Benutzerkonto gestartet, unter dem der Dienst des Administrationsservers ausgeführt wird.

Schritt 9. Installation starten

Dies ist der abschließende Schritt des Assistenten. In diesem Schritt wurde die **Aufgabe zur Remote-Installation** erfolgreich erstellt und konfiguriert.

Die Variante **Aufgabe nach Abschluss des Assistenten starten** ist standardmäßig nicht ausgewählt. Wenn Sie diese Option auswählen, startet die **Aufgabe zur Remote-Installation** sofort nach Abschluss des Assistenten. Wenn Sie diese Option nicht auswählen, startet die **Aufgabe zur Remote-Installation** nicht. Sie können diese Aufgabe später manuell starten.

Klicken Sie auf **Uhrzeit der Verschlüsselung**, um den letzten Schritt des Assistenten für die Bereitstellung des Schutzes abzuschließen.

Konfigurieren des Administrationsservers

Dieser Abschnitt beschreibt den Konfigurationsprozess und die Eigenschaften des Kaspersky Security Center Linux Administrationsservers.

Verbindung zwischen Kaspersky Security Center 14 Web Console und Administrationsserver anpassen

So legen Sie die Verbindungsports des Administrationsservers fest:

1. Klicken Sie im oberen Bereich des Bildschirms auf das Symbol **Einstellungen** ( ) neben dem Namen des erforderlichen Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

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

Die Anwendung zeigt die wichtigsten Verbindungseinstellungen des ausgewählten Servers an.

Konfiguration einer Allow-Liste mit IP-Adressen für die Anmeldung bei Kaspersky Security Center

Standardmäßig können sich Benutzer auf jedem Gerät, auf dem sie die Kaspersky Security Center 14 Web Console (im Folgenden "Web Console" genannt) öffnen können, bei Kaspersky Security Center anmelden. Sie können den Administrationsserver jedoch auch so konfigurieren, dass Benutzer nur von Geräten mit zugelassenen IP-Adressen eine Verbindung zu ihm herstellen dürfen. Selbst wenn ein Eindringling an die Anmeldedaten eines Benutzerkontos von Kaspersky Security Center gelangt, kann er sich in diesem Fall nicht bei Kaspersky Security Center anmelden, da die IP-Adresse des Geräts des Eindringlings nicht auf der Allow-Liste steht.

Die IP-Adresse wird überprüft, wenn sich ein Benutzer an Kaspersky Security Center anmeldet oder eine Anwendung ausführt, die mit dem Administrationsserver über Kaspersky Security Center OpenAPI interagiert. In so einem Moment versucht das Gerät des Benutzers, eine Verbindung mit dem Administrationsserver herzustellen. Befindet sich die IP-Adresse des Geräts nicht auf der Allow-Liste, tritt ein Authentifizierungsfehler auf und das Ereignis KLAUD_EV_SERVERCONNECT benachrichtigt Sie darüber, dass eine Verbindung mit dem Administrationsserver abgelehnt wurde.

Anforderungen an eine Allow-Liste mit IP-Adressen

IP-Adressen werden nur überprüft, wenn die folgenden Programme versuchen, sich mit dem Administrationsserver zu verbinden:

- Server der Web Console

  Wenn Sie sich über die Web Console bei Kaspersky Security Center anmelden, können Sie mit den Standardwerkzeugen des Betriebssystems eine Firewall auf dem Gerät konfigurieren, auf dem der Server der Web Console installiert ist. Wenn anschließend jemand versucht, sich von einem Gerät aus an Kaspersky Security Center anzumelden, wobei der Server der Web Console auf einem anderen Gerät installiert ist, hilft eine Firewall, die Eindringlinge abzuweisen.

- Programme, die mittels klakaut-Automatisierungsobjekten mit dem Administrationsserver interagieren

- Programme, die mittels OpenAPI mit dem Administrationsserver interagieren, z. B. Kaspersky Anti Targeted Attack Platform oder Kaspersky Security for Virtualization

Geben Sie daher Adressen der Geräte an, auf denen die oben aufgeführten Programme installiert sind.

Sie können sowohl IPv4- als auch IPv6-Adressen angeben. Sie können keine IP-Adressbereiche angeben.

So erstellen Sie eine Allow-Liste mit IP-Adressen

Wenn Sie zuvor noch keine Allow-Liste erstellt haben, folgen Sie den nachstehenden Anweisungen.

So erstellen Sie die Allow-Liste mit IP-Adressen zur Anmeldung an Kaspersky Security Center:

1. Führen Sie auf dem Gerät des Administrationsservers die Eingabeaufforderung unter einem Konto mit Administratorrechten aus.

2. Ändern Sie das aktuelle Verzeichnis des Installationsordners von Kaspersky Security Center (üblicherweise /opt/kaspersky/ksc64/sbin).

3. Geben Sie den folgenden Befehl mit Administratorrechten ein:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP-Adressen>" -t s`

   Geben Sie IP-Adressen an, die den oben aufgeführten Anforderungen entsprechen. Mehrere IP-Adressen müssen durch ein Semikolon getrennt werden.

   Beispiel, um nur einem Gerät die Verbindung mit dem Administrationsserver zu erlauben:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   Beispiel, um mehreren Geräten die Verbindung mit dem Administrationsserver zu erlauben:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s`

4. Starten Sie den Dienst des Administrationsservers neu.

Dem Syslog-Ereignisprotokoll auf dem Administrationsserver können Sie entnehmen, ob Sie die Allow-Liste mit IP-Adressen erfolgreich konfiguriert haben.

So ändern Sie eine Allow-Liste mit IP-Adressen

Sie können eine Allow-Liste auf gleiche Weise ändern, wie Sie es bei der erstmaligen Erstellung getan haben. Führen Sie daher denselben Befehl aus und geben Sie eine neue Allow-Liste an:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP-Adressen>" -t s
```

Wenn Sie einige IP-Adressen aus der Zulassungsliste löschen möchten, erstellen Sie diese neu. Ihre Allow-Liste enthält beispielsweise die folgenden IP-Adressen: 192.0.2.0; 198.51.100.0 und 203.0.113.0. Sie möchten die IP-Adresse 198.51.100.0 aus der Liste löschen. Geben Sie dafür den folgenden Befehl in die Eingabeaufforderung ein:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

Stellen Sie sicher, den Dienst des Administrationsservers neu zu starten.

Zurücksetzen einer konfigurierten Allow-Liste mit IP-Adressen

So setzen Sie eine bereits konfigurierte Allow-Liste mit IP-Adressen zurück:

1. Geben Sie den folgenden Befehl mit Administratorrechten in die Eingabeaufforderung ein:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`

2. Starten Sie den Dienst des Administrationsservers neu.

Anschließend werden IP-Adressen nicht mehr überprüft.

Protokoll der Verbindungen zum Administrationsserver anzeigen

Der Verlauf der Verbindungen und Versuche, während des Betriebs eine Verbindung mit dem Administrationsserver herzustellen, können in einer Protokolldatei gespeichert werden. Mit den Informationen in der Datei können Sie nicht nur Verbindungen innerhalb Ihrer Netzwerkinfrastruktur verfolgen, sondern auch nicht autorisierte Versuche, auf den Server zuzugreifen.

So protokollieren Sie die Ereignisse der Verbindung zum Administrationsserver:

1. Klicken Sie im Hauptfenster der Anwendung neben dem Namen des benötigten Administrationsservers auf das Symbol **Einstellungen** ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

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

3. Aktivieren Sie die Option **Verbindungsereignisse des Administrationsservers protokollieren**.

Alle weiteren Ereignisse eingehender Verbindungen zum Administrationsserver, Authentifizierungsergebnisse und SSL-Fehler werden in der Datei %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog gespeichert.

Beschränkung der maximalen Anzahl der Ereignisse in der Ereignis-Datenverwaltung

Im Eigenschaftenfenster des Administrationsservers können Sie im Abschnitt **Ereignis-Datenverwaltung** die Einstellungen für das Speichern der Ereignisse in der Datenbank des Servers anpassen: Anzahl der Einträge über Ereignisse und Speicherdauer der Einträge beschränken. Wenn Sie die maximale Anzahl der Ereignisse angeben, berechnet die Anwendung einen ungefähren Wert des für die angegebene Zahl benötigten Speicherplatzes. Sie können diese ungefähre Berechnung verwenden, um zu überprüfen, ob Sie ausreichen freien Platz auf dem Laufwerk haben, um einen Überlauf der Datenbank zu vermeiden. Standardmäßig umfasst die Datenbank des Administrationsservers 400.000 Ereignisse. Die empfohlene Maximalgröße der Datenbank liegt bei 45 Millionen Ereignissen.

Wenn die Anzahl der Ereignisse in der Datenbank den vom Administrator angegebenen Maximalwert erreicht, werden die ältesten Ereignisse vom Programm gelöscht und durch neue überschrieben. Wenn der Administrationsserver alte Ereignisse löscht, kann er keine neuen Ereignisse in der Datenbank speichern. Während dieser Zeitspanne werden Informationen über abgelehnte Ereignisse in das Ereignisprotokoll "Kaspersky" geschrieben. Die neuen Ereignisse werden in die Warteschlange verschoben und dann in der Datenbank gespeichert, nachdem der Löschvorgang abgeschlossen wurde.

Um die Anzahl der Ereignisse, die in der Ereignis-Datenverwaltung des Administrationsservers gespeichert werden können, zu begrenzen, gehen Sie wie folgt vor:

1. Klicken Sie im oberen Bereich des Bildschirms auf das Symbol **Einstellungen** ( ) neben dem Namen des erforderlichen Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Ereignis-Datenverwaltung** aus. Geben Sie die maximale Anzahl von Ereignissen an, die in der Datenbank gespeichert sind.

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

Daten des Administrationsservers sichern, kopieren und wiederherstellen (Backup / Recovery)

Die Datensicherung ermöglicht es Ihnen, den Administrationsserver ohne Datenverlust von einem Gerät auf ein anderes zu übertragen. Durch das Backup können Sie die Daten wiederherstellen, wenn Sie die Datenbank des Administrationsservers auf ein anderes Gerät verschieben oder ein Upgrade auf eine neuere Version von Kaspersky Security Center durchführen.

Beachten Sie, dass die installierten Verwaltungs-Plug-Ins nicht gesichert werden. Nachdem Sie die Daten des Administrationsservers aus einer Sicherungskopie wiederhergestellt haben, müssen Sie Plug-ins für die verwalteten Programme herunterladen und neu installieren.

Sie können eine Backup-Kopie der Daten des Administrationsservers auf eine der folgenden Weisen erstellen:

- Erstellen und Ausführen einer Datensicherungsaufgabe über Kaspersky Security Center 14 Web Console.
- Das Tool klbackup auf einem Gerät mit dem installierten Administrationsserver starten. Dieses Tool gehört zum Lieferumfang von Kaspersky Security Center. Es befindet sich nach der Installation des Administrationsservers im Stammverzeichnis des Zielordners, der bei der Programm-Installation angegeben wurde (gewöhnlich im Ordner /opt/kaspersky/ksc64/sbin/klbackup).

In der Backup-Kopie der Daten des Administrationsservers werden folgende Daten gespeichert:

- Datenbank des Administrationsservers (Richtlinien, Aufgaben, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse).
- Konfigurationsdaten über die Struktur der Administrationsgruppen und Client-Geräte.
- Speicherort der Programmpakete für die Remote-Installation.
- Zertifikat des Administrationsservers.

Die Wiederherstellung von Daten des Administrationsservers ist nur mithilfe des Hilfsprogramms klbackup möglich.

Sicherungsaufgabe für die Daten des Administrationsserver erstellen

Sicherungsaufgaben gehören zu den Aufgaben des Administrationsservers und werden vom Schnellstartassistenten erstellt. Wenn die vom Schnellstartassistenten erstellte Aufgabe zum Anlegen eines Backups gelöscht wurde, können Sie diese manuell erstellen.

Die Aufgabe *Backup der Daten des Administrationsservers anlegen* kann nur einmal erstellt werden. Wenn die Backup-Aufgabe für die Daten des Administrationsservers für den Administrationsserver bereits erstellt wurde, wird sie im Fenster für die Auswahl des Aufgabentyps nicht angezeigt.

Um eine Aufgabe zum Anlegen eines Backups des Administrationsservers zu erstellen, gehen Sie wie folgt vor:

1. Gehen Sie zu **GERÄTE** → **AUFGABEN**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent zum Hinzufügen von Aufgaben wird gestartet.
3. Wählen Sie auf der ersten Seite des Assistenten in der Liste **Programm** die Option **Hersteller** und in der Liste **Aufgabentyp** die Option **Backup der Daten des Administrationsservers anlegen** aus.
4. Geben Sie auf der entsprechenden Seite des Assistenten die folgenden Informationen an:
   - Ordner zum Speichern der Backup-Kopien
   - Kennwort für das Backup (optional)
   - Maximale Anzahl zu speichernder Backup-Kopien
5. 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.
6. Klicken Sie auf die Schaltfläche **Fertigstellen**.

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

Tool zur Sicherung- und Wiederherstellung der Daten (klbackup)

Sie können die Daten des Administrationsservers mittels des Tools klbackup, welches im Lieferumfang von Kaspersky Security Center enthalten ist, zum Zweck eines Backups und späterer Wiederherstellung kopieren.

Hilfsprogramm klbackup kann in zwei Modi arbeiten:

- Interaktiv
- Nicht interaktiv

Daten im interaktiven Modus sichern, kopieren und wiederherstellen

Um eine Backup-Kopie der Daten des Administrationsservers im interaktiven Modus zu erstellen, gehen Sie wie folgt vor:

1. Führen Sie das Dienstprogramm klbackup aus, das sich im Installationsordner von Kaspersky Security Center befindet (gewöhnlich im Ordner /opt/kaspersky/ksc64/sbin/klbackup).

   Der Backup- und Wiederherstellungsassistent wird gestartet.

2. Wählen Sie im ersten Fenster des Assistenten die Option **Anlegen eines Backups der Daten des Administrationsservers** aus.

   Bei aktivierter Option **Nur das Zertifikat des Administrationsservers sichern und wiederherstellen** wird nur die Backup-Kopie des Zertifikats des Administrationsservers gespeichert.

   Klicken Sie auf die Schaltfläche **Weiter**.

3. Geben Sie im nächsten Fenster des Assistenten ein Kennwort und einen Zielordner für das Backup an und klicken Sie anschließend auf die Schaltfläche **Weiter**, um das Erstellen des Backups zu starten.

Um Daten des Administrationsservers im interaktiven Modus wiederherzustellen, gehen Sie wie folgt vor:

1. Führen Sie das Dienstprogramm klbackup aus, das sich im Installationsordner von Kaspersky Security Center befindet (gewöhnlich im Ordner /opt/kaspersky/ksc64/sbin/klbackup). Starten Sie das Tool unter demselben Benutzerkonto, mit dem Sie auch den Administrationsserver installiert haben.

   Der Backup- und Wiederherstellungsassistent wird gestartet.

2. Wählen Sie im ersten Fenster des Assistenten die Option **Wiederherstellen der Daten des Administrationsservers** aus.

   Wenn Sie die Option **Nur das Zertifikat des Administrationsservers sichern und wiederherstellen** auswählen, wird nur das Zertifikat des Administrationsservers wiederhergestellt.

   Klicken Sie auf die Schaltfläche **Weiter**.

3. Gehen Sie im Assistenten im Fenster **Einstellungen für Wiederherstellung** folgendermaßen vor:

   - Geben Sie den Ordner an, der die Backup-Kopie der Daten des Administrationsservers enthält. Stellen Sie sicher, dass die Datei backup.zip heißt.

   - Geben Sie das Kennwort ein, das beim Verschieben ins Backup festgelegt wurde.

     Beim Wiederherstellen der Daten muss dasselbe Kennwort eingegeben werden wie beim Verschieben ins Backup. Wenn der Pfad zum freigegebenen Ordner nach dem Verschieben ins Backup verändert wird, muss nach der Wiederherstellung der Daten die Funktion jener Aufgaben überprüft werden, bei denen die wiederhergestellten Daten verwendet werden (Wiederherstellungsaufgaben, Remote-Installation). Erforderlichenfalls müssen die Einstellungen dieser Aufgaben geändert werden. Während der Wiederherstellung von Daten aus dem Backup darf der freigegebene Ordner des Administrationsservers von niemandem verwendet werden. Das Benutzerkonto, unter dem das Tool klbackup gestartet wird, muss über vollen Zugriff auf den freigegebenen Ordner verfügen.

4. Klicken Sie auf die Schaltfläche **Weiter** für die Wiederherstellung von Daten.

Daten im nicht-interaktiven Modus sichern, kopieren und wiederherstellen

Um eine Backup-Kopie der Daten zu erstellen oder Daten des Administrationsservers im nicht interaktiven Modus wiederherzustellen,

starten Sie aus der Befehlszeile des Geräts, auf dem der Administrationsserver installiert ist, das Tool klbackup mit der erforderlichen Auswahl an Schlüsseln.

Die Befehlszeilensyntax des Tools lautet:

```
klbackup -path BACKUP_PATH [-logfile LOGFILE] [-use_ts]|[-restore] [-password PASSWORD]
[-online]
```

Wenn in der Befehlszeile des Tools klbackup kein Kennwort eingegeben wird, fragt das Tool das Kennwort interaktiv ab.

Die Schlüssel weisen folgende Bedeutung auf:

- `-path BACKUP_PATH` – Daten im Ordner BACKUP_PATH speichern/zum Wiederherstellen Daten aus dem Ordner BACKUP_PATH (Pflichtparameter) verwenden.
- `-logfile LOGFILE` – Bericht über das Kopieren oder Wiederherstellen der Daten des Administrationsservers speichern.

  Das Benutzerkonto der Server-Datenbank und das Tool klbackup müssen über die Berechtigung zum Ändern der Daten im Ordner BACKUP_PATH verfügen.
- `-use_ts` – Beim Speichern die Daten in einen Unterordner im Ordner BACKUP_PATH kopieren, dessen Name das aktuelle Systemdatum und die aktuelle Systemuhrzeit im Format `klbackup JJJJ-MM-TT # HH-MM-SS` enthält. Wenn der Schlüssel nicht eingegeben wurde, werden die Angaben im Stammverzeichnis des Ordners BACKUP_PATH abgelegt.

  Wenn Sie versuchen, die Informationen in einem Ordner zu speichern, in dem bereits eine Backup-Kopie vorhanden ist, erscheint eine Fehlermeldung. Die Informationen werden nicht aktualisiert.

  Mit dem Schlüssel `-use_ts` kann ein Datenarchiv des Administrationsservers angelegt werden. Wenn z. B. mit dem Schlüssel `-path` der Ordner `C:\KLBackups` vorgegeben wurde, werden im Ordner `klbackup 2022/6/19 # 11-30-18` Informationen über den Status des Administrationsservers mit Stand vom 19. Juni 2022 um 11 Uhr, 30 Minuten und 18 Sekunden abgelegt.
- `-restore` – Daten des Administrationsservers wiederherstellen. Die Wiederherstellung der Daten erfolgt anhand der Informationen, die im Ordner BACKUP_PATH liegen. Wenn der Schlüssel fehlt, wird die Backup-Kopie im Ordner BACKUP_PATH erstellt.
- `-password PASSWORD` – Zertifikat des Administrationsservers speichern oder wiederherstellen. Für die Verschlüsselung und Entschlüsselung des Zertifikats wird das Kennwort verwendet, das mit dem Parameter PASSWORD vorgegeben wurde.

  Ein vergessenes Kennwort kann nicht wiederhergestellt werden. Es gibt keine Kennwortanforderungen. Die Kennwortlänge ist unbegrenzt und eine Länge von Null (kein Kennwort) ist ebenfalls möglich.

  Beim Wiederherstellen der Daten muss dasselbe Kennwort eingegeben werden wie beim Verschieben ins Backup. Wenn der Pfad zum freigegebenen Ordner nach dem Verschieben ins Backup verändert wird, muss nach der Wiederherstellung der Daten die Funktion jener Aufgaben überprüft werden, bei denen die wiederhergestellten Daten verwendet werden (Wiederherstellungsaufgaben, Remote-Installation). Erforderlichenfalls müssen die Einstellungen dieser Aufgaben geändert werden. Während der Wiederherstellung von Daten aus dem Backup darf der freigegebene Ordner des Administrationsservers von niemandem verwendet werden. Das Benutzerkonto, unter dem das Tool klbackup gestartet wird, muss über vollen Zugriff auf den freigegebenen Ordner verfügen.
- `-online` – Daten des Administrationsservers mithilfe der Erstellung eines Volume-Snapshots sichern, um die Offline-Zeit des Administrationsservers zu reduzieren. Wenn Sie das Tool zur Wiederherstellung von Daten verwenden, wird diese Option ignoriert.

Den Administrationsserver und einen Datenbankserver auf ein anderes Gerät verschieben

Wenn Sie den Administrationsserver auf einem neuen Gerät verwenden müssen, können Sie ihn auf eine der folgenden Arten verschieben:

- Verschieben Sie den Administrationsserver und den Datenbankserver auf ein neues Gerät.
- Belassen Sie den Datenbankserver auf dem bisherigen Gerät und verschieben Sie nur den Administrationsserver auf ein neues Gerät.

Um den Administrationsserver und den Datenbankserver auf ein neues Gerät zu verschieben:

1. Erstellen Sie auf dem bisherigen Gerät ein Backup der Daten des Administrationsservers.

   Dazu können Sie entweder die Datensicherungsaufgabe über Kaspersky Security Center 14 Web Console ausführen oder das Dienstprogramm klbackup ausführen.

2. Wählen Sie ein neues Gerät aus, auf dem der Administrationsserver installiert werden soll. Stellen Sie sicher, dass die Hardware und Software des ausgewählten Gerätes den Anforderungen für den Administrationsserver, für Kaspersky Security Center 14 Web Console und für den Administrationsagenten entsprechen. Überprüfen Sie außerdem, ob die auf dem Administrationsserver verwendeten Ports verfügbar sind.

3. Installieren Sie auf dem neuen Gerät das Datenbankverwaltungssystem (DBMS), das vom Administrationsserver verwenden wird.

   Berücksichtigen Sie bei der Auswahl eines DBMS die Anzahl der vom Administrationsserver verwalteten Geräte.

4. Installieren Sie den Administrationsserver auf dem neuen Gerät.

   Hinweis: Wenn Sie den Datenbankserver auf das neue Gerät verschieben, müssen Sie die lokale Adresse als IP-Adresse des Gerätes angeben, auf dem die Datenbank installiert ist (Element "h" in der Anweisung Kaspersky Security Center installieren). Wenn Sie den Datenbankserver auf dem bisherigen Gerät belassen müssen, geben Sie die IP-Adresse des bisherigen Geräts im Element "h" der Anweisung Kaspersky Security Center installieren an.

5. Stellen Sie nach Abschluss der Installation die Administrationsserver-Daten auf dem neuen Gerät mithilfe des Dienstprogramms klbackup wieder her.

   > Wenn Sie als DBMS auf dem vorherigen und neuen Gerät SQL Server verwenden, beachten Sie, dass die auf dem neuen Gerät installierte Version von SQL Server mit der auf dem vorherigen Gerät installierten Version von SQL Server identisch oder höher sein muss. Andernfalls können Sie die Daten des Administrationsservers auf dem neuen Gerät nicht wiederherstellen.

6. Öffnen Sie die Kaspersky Security Center 14 Web Console und stellen Sie eine Verbindung zum Administrationsserver her.

7. Überprüfen Sie, ob alle Client-Geräte mit dem Administrationsserver verbunden sind.

8. Deinstallieren Sie den Administrationsserver und den Datenbankserver vom bisherigen Gerät.

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 Hauptfenster der Anwendung neben dem Namen des benötigten Administrationsservers auf das Symbol **Einstellungen** ( ).
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. Der virtuelle Administrationsserver wird die Geräte dieser ausgewählten Gruppe (einschließlich der Untergruppen) verwalten.
4. Klicken Sie in der Menüleiste auf **Neuer virtueller Administrationsserver**.
5. Legen Sie auf der nächsten Seite die Eigenschaften des neuen virtuellen Administrationsservers fest:
   - **Name des virtuellen Administrationsservers**.
   - **Verbindungsadresse des Administrationsservers**

     Sie können den Namen oder die IP-Adresse Ihres Administrationsservers angeben.
6. Wählen Sie aus der Benutzerliste den Administrator des virtuellen Administrationsservers aus. Bei Bedarf können Sie vor der Zuweisung der Administratorrolle eines der vorhandenen Benutzerkonten bearbeiten oder ein neues Benutzerkonto erstellen.
7. Klicken Sie auf die Schaltfläche **Speichern**.

Der neue virtuelle Administrationsserver wird erstellt, zur Administrationsgruppe hinzugefügt und auf der Registerkarte **Administrationsserver** angezeigt.

Wenn Sie in der Kaspersky Security Center 14 Web Console mit Ihrem primären Administrationsserver verbunden sind und keine Verbindung zu einem virtuellen Administrationsserver, der von einem sekundären Administrationsserver verwaltet wird, herstellen können, haben Sie folgende Möglichkeiten:

- Ändern Sie die vorhandene Installation von Kaspersky Security Center 14 Web Console, um den sekundären Server zur Liste der vertrauenswürdigen Administrationsserver hinzuzufügen. Anschließend können Sie sich in Kaspersky Security Center 14 Web Console mit dem virtuellen Administrationsserver verbinden.

1. Führen Sie auf dem Gerät, auf dem Kaspersky Security Center 14 Web Console installiert ist, die ausführbare Datei ksc-web-console.<Versionsnummer>.<Build-Nummer>.exe unter einem Benutzerkonto mit Administratorrechten aus.
2. Der Installationsassistent wird gestartet.
3. Wählen Sie auf der ersten Seite des Assistenten die Option **Upgrade** aus.
4. Wählen Sie auf der Seite **Änderungstyp** die Option **Verbindungseinstellungen ändern** aus.
5. Fügen Sie auf der Seite **Vertrauenswürdige Administrationsserver** den gewünschten sekundären Administrationsserver hinzu.
6. Klicken Sie auf der letzten Seite des Assistenten auf **Ändern**, um die neuen Einstellungen zu übernehmen.
7. Nach dem erfolgreichen Abschluss der Neukonfigurierung des Programms klicken Sie auf die Schaltfläche **Fertigstellen**.

- Verwenden Sie die Kaspersky Security Center 14 Web Console, um eine direkte Verbindung mit dem sekundären Administrationsserver herzustellen auf dem der virtuelle Server erstellt wurde. Anschließend können Sie in Kaspersky Security Center 14 Web Console zum virtuellen Administrationsserver wechseln.
- Verwenden Sie die MMC-basierte Verwaltungskonsole, um eine direkte Verbindung mit dem virtuellen Server herzustellen.

Administrationsserver-Hierarchie

Beim MSP kann mehr als ein Administrationsserver vorhanden sein. Die Verwaltung mehrerer vereinzelter Administrationsserver ist unpraktisch, deshalb es ist zweckmäßig, sie in einer Hierarchie zusammenzufassen.

In einer Hierarchie kann der Linux-Administrationsserver von Kaspersky Security Center nur als sekundärer Server fungieren, der von einem primären Administrationsserver des Windows-basierten Kaspersky Security Center oder Kaspersky Security Center Cloud Console verwaltet wird.

Eine "Primär/Sekundär"-Konfiguration für zwei Administrationsserver bietet die folgenden Möglichkeiten:

- Der sekundäre Administrationsserver erbt vom primären Administrationsserver die Richtlinien und Aufgaben, wobei duplizierte Einstellungen entfernt werden.
- Die Geräteauswahlen auf dem primären Administrationsserver können Geräte der sekundären Administrationsserver einschließen.
- Die Berichte auf dem primären Administrationsserver können Daten (einschließlich ausführlicher Informationen) der sekundären Administrationsserver einschließen.

Hierarchie der Administrationsserver erstellen: einen sekundären Administrationsserver hinzufügen

In einer Hierarchie kann der Linux-Administrationsserver von Kaspersky Security Center nur als sekundärer Server fungieren, der von einem primären Administrationsserver des Windows-basierten Kaspersky Security Center oder Kaspersky Security Center Cloud Console verwaltet wird.

Sekundären Administrationsserver hinzufügen (Ausführung auf dem zukünftigen primären Administrationsserver)

Sie können einen Administrationsserver als sekundären Administrationsserver hinzufügen und so eine Hierarchie vom Typ "primärer/sekundärer" festlegen.

Um einen sekundären Administrationsserver hinzuzufügen, der mit Kaspersky Security Center 14 Web Console verbunden werden kann, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der Port 13000 des zukünftigen primären Administrationsservers für die Annahme von Verbindungen von sekundären Administrationsservern verfügbar ist.
2. Klicken Sie auf dem zukünftigen primären Administrationsserver auf das Symbol **Einstellungen** ( ).
3. Wechseln Sie auf der folgenden Eigenschaftenseite auf die Registerkarte **Administrationsserver**.
4. Wählen Sie das Kontrollkästchen neben der Administrationsgruppe aus, zu der Sie den virtuellen Administrationsserver hinzufügen möchten.
5. Klicken Sie in der Menüleiste auf **Sekundären Administrationsserver verbinden**.

   Der Assistent zum Verbinden eines sekundären Administrationsservers wird gestartet.
6. 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.

   - **SSL-Port des Administrationsservers**

     Geben Sie die Nummer des SSL-Ports auf dem primären Administrationsserver an. Standardmäßig ist Portnummer 13000 angegeben.

   - **API-Port des Administrationsservers**

     Geben Sie die Nummer des Ports auf dem primären Aministrationsserver an, über den Verbindungen über OpenAPI eingehen sollen. Standardmäßig ist Portnummer 13299 angegeben.

   - **Primären Administrationsserver mit sekundärem Administrationsserver in der DMZ verbinden**

Wählen Sie diese Option, wenn sich der sekundäre Administrationsserver in einer demilitarisierten Zone (DMZ) befindet.

Wenn diese Option ausgewählt ist, initiiert der primäre Administrationsserver die Verbindung mit dem sekundären Administrationsserver. Andernfalls verbindet sich der sekundäre Administrationsserver mit dem primären Administrationsserver.

- **Proxyserver verwenden**

  Wählen Sie diese Option, wenn die Verbindung zum sekundären Administrationsserver über einen Proxyserver hergestellt wird.

  In diesem Fall müssen Sie außerdem die folgenden Einstellungen des Proxyservers angeben:

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

7. Folgen Sie den weiteren Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird die Hierarchie "primärer / sekundärer Server" gebildet. Die Verbindung zwischen dem primären und dem sekundären Administrationsserver wird über Port 13000 hergestellt. Die vom primären Administrationsserver bereitgestellten Aufgaben und Richtlinien werden abgerufen und angewendet. Der sekundäre Administrationsserver wird auf dem primären Administrationsserver in der Administrationsgruppe angezeigt, in der er hinzugefügt wurde.

Sekundären Administrationsserver hinzufügen (Ausführung auf dem zukünftigen sekundären Administrationsserver)

Wenn Sie keine Verbindung zum zukünftigen sekundären Administrationsserver aufbauen konnten (da dieser z. B. vorübergehend getrennt oder nicht verfügbar war), können Sie trotzdem einen sekundären Administrationsserver hinzufügen.

Um einen Administrationsserver, der nicht für die Verbindung über Kaspersky Security Center 14 Web Console verfügbar ist, als sekundären Server hinzuzufügen, gehen Sie wie folgt vor:

1. Senden Sie die Zertifikatsdatei des zukünftigen primären Administrationsservers an den Systemadministrator des Büros, in dem sich der zukünftige sekundäre Administrationsserver befindet. (Sie können die Datei z. B. auf einem externen Gerät wie einem Flash-Laufwerk speichern oder per E-Mail senden.)

   Die Zertifikatsdatei befindet sich auf dem zukünftigen primären Administrationsserver unter /var/opt/kaspersky/klnagent_srv/1093/cert/.

2. Bitten Sie den Systemadministrator, der für den zukünftigen sekundären Administrationsserver zuständig ist, wie folgt vorzugehen:

   a. Klicken Sie auf das Symbol **Einstellungen** ( ).

   b. Wechseln Sie auf der nächsten Seite mit Eigenschaften zum Abschnitt **Hierarchie der Administrationsserver** auf der Registerkarte **Allgemein**.

   c. Wählen Sie die Option **Dieser Administrationsserver ist in der Server-Hierarchie sekundär** aus.

d. Geben Sie im Feld **Adresse des primären Administrationsservers** den Netzwerknamen des zukünftigen primären Administrationsservers an.

e. Wählen Sie die zuvor gespeicherte Zertifikatsdatei des zukünftigen primären Administrationsservers aus, indem Sie auf **Durchsuchen** klicken.

f. Aktivieren Sie bei Bedarf das Kontrollkästchen **Primären Administrationsserver mit sekundärem Administrationsserver in der DMZ verbinden**.

g. Wenn die Verbindung mit dem zukünftigen sekundären Administrationsserver über einen Proxyserver hergestellt wird, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben Sie die Verbindungseinstellungen ein.

h. Klicken Sie auf die Schaltfläche **Speichern**.

Die "primär/sekundär"-Hierarchie wird gebildet. Der primäre Administrationsserver nimmt über Port 13000 Verbindungen vom sekundären Administrationsserver an. Die vom primären Administrationsserver bereitgestellten Aufgaben und Richtlinien werden abgerufen und angewendet. Der sekundäre Administrationsserver wird auf dem primären Administrationsserver in der Administrationsgruppe angezeigt, in der er hinzugefügt wurde.

Liste mit sekundären Administrationsservern anzeigen

So zeigen Sie eine Liste mit sekundären (einschl. virtuellen) Administrationsservern an:

Klicken Sie im Hauptanwendungsfenster auf den Namen des Administrationsservers neben dem Symbol **Einstellungen** ( ).

Eine Dropdown-Liste mit sekundären (einschl. virtuellen) Administrationsservern wird angezeigt.

Sie können auf den Namen eines dieser Administrationsserver klicken, um zu ihm zu wechseln.

Die Administrationsgruppen werden ebenfalls angezeigt, sind jedoch ausgegraut und stehen in diesem Menü nicht zur Verwaltung zur Verfügung.

Wenn Sie in der Kaspersky Security Center 14 Web Console mit Ihrem primären Administrationsserver verbunden sind und keine Verbindung zu einem virtuellen Administrationsserver, der von einem sekundären Administrationsserver verwaltet wird, herstellen können, haben Sie folgende Möglichkeiten:

- Ändern Sie die vorhandene Installation von Kaspersky Security Center 14 Web Console, um den sekundären Server zur Liste der vertrauenswürdigen Administrationsserver hinzuzufügen. Anschließend können Sie sich in Kaspersky Security Center 14 Web Console mit dem virtuellen Administrationsserver verbinden.

1. Führen Sie auf dem Gerät, auf dem Kaspersky Security Center 14 Web Console installiert ist, die ausführbare Datei ksc-web-console.<Versionsnummer>.<Build-Nummer>.exe unter einem Benutzerkonto mit Administratorrechten aus.
2. Der Installationsassistent wird gestartet.
3. Wählen Sie auf der ersten Seite des Assistenten die Option **Upgrade** aus.
4. Wählen Sie auf der Seite **Änderungstyp** die Option **Verbindungseinstellungen ändern** aus.
5. Fügen Sie auf der Seite **Vertrauenswürdige Administrationsserver** den gewünschten sekundären Administrationsserver hinzu.
6. Klicken Sie auf der letzten Seite des Assistenten auf **Ändern**, um die neuen Einstellungen zu übernehmen.
7. Nach dem erfolgreichen Abschluss der Neukonfigurierung des Programms klicken Sie auf die Schaltfläche **Fertigstellen**.

- Verwenden Sie die Kaspersky Security Center 14 Web Console, um eine direkte Verbindung mit dem sekundären Administrationsserver herzustellen auf dem der virtuelle Server erstellt wurde. Anschließend können Sie in Kaspersky Security Center 14 Web Console zum virtuellen Administrationsserver wechseln.
- Verwenden Sie die MMC-basierte Verwaltungskonsole, um eine direkte Verbindung mit dem virtuellen Server herzustellen.

Aktivieren des Benutzerkonten-Schutzes vor unbefugten Änderungen

Sie können eine zusätzliche Option aktivieren, um ein Benutzerkonto vor unbefugten Änderungen zu schützen. Wenn diese Option aktiviert ist, muss sich der Benutzer mit Änderungsrechten autorisieren, um die Benutzerkonto-Einstellungen zu ändern.

Um den Benutzerkonten-Schutz vor unbefugten Änderungen zu aktivieren oder zu deaktivieren:

1. Gehen Sie zu **BENUTZER UND ROLLEN** → **BENUTZER**.
2. Klicken Sie auf den Namen des internen Benutzerkontos, für das Sie den Benutzerkonten-Schutz vor nicht autorisierten Änderungen anpassen möchten.
3. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Sicherheit für die Authentifizierung**.
4. Wählen Sie auf der Registerkarte **Sicherheit für die Authentifizierung** die Option **Authentifizierung verlangen, um die Berechtigung zum Ändern von Benutzerkonten zu überprüfen**, wenn Sie jedes Mal Anmeldedaten anfordern möchten, sobald Benutzerkonto-Einstellungen geändert oder bearbeitet werden. Wählen Sie andernfalls die Option **Benutzern das Ändern des Kontos ohne zusätzliche Authentifizierung erlauben**.
5. Klicken Sie auf **Speichern**.

Zwei-Faktor-Authentifikation

In diesem Abschnitt wird beschrieben, wie Sie die Zwei-Faktor-Authentifikation verwenden können, um das Risiko eines nicht autorisierten Zugriffs auf die Kaspersky Security Center 14 Web Console zu verringern.

Szenario: Konfigurieren der Zwei-Faktor-Authentifikation für alle Benutzer

In diesem Szenario wird beschrieben, wie Sie die Zwei-Faktor-Authentifikation für alle Benutzer aktivieren und wie Benutzerkonten von der Zwei-Faktor-Authentifikation ausschließen. Wenn Sie die Zwei-Faktor-Authentifikation für Ihr Benutzerkonto nicht aktiviert haben, bevor Sie es für andere Benutzer aktivieren, öffnet die Anwendung zunächst das Fenster zur Aktivierung der Zwei-Faktor-Authentifikation für Ihr Konto. In diesem Szenario wird außerdem beschrieben, wie Sie die Zwei-Faktor-Authentifikation für Ihr eigenes Benutzerkonto aktivieren.

Wenn Sie die Zwei-Faktor-Authentifikation für Ihr Benutzerkonto aktiviert haben, können Sie mit der Aktivierung der Zwei-Faktor-Authentifikation für alle Benutzer fortsetzen.

Erforderliche Komponenten

Vor dem Start:

- Stellen Sie sicher, dass Ihr Benutzerkonto über die Berechtigung "Objekt-ACL ändern" für den Funktionsbereich **Allgemeine Funktionen: Benutzerrechte** verfügt, um die Sicherheitseinstellungen für andere Benutzerkonten zu ändern.
- Stellen Sie sicher, dass die anderen Benutzer des Administrationsservers eine Authentifizierungs-App auf ihren Geräten installieren.

Schritte

Das Aktivieren der Zwei-Faktor-Authentifikation für alle Benutzer erfolgt schrittweise:

1. **Installation einer Authentifizierungs-App auf einem Gerät**

   Sie können Google Authenticator, Microsoft Authenticator oder eine andere Authentifizierungs-App installieren, die den Algorithmus für zeitbasierte Einmalkennwörter unterstützt.

2. **Synchronisation der Zeit der Authentifizierungs-App mit der Zeit des Gerätes, auf dem der Administrationsserver installiert ist**

   Stellen Sie sicher, dass die in der Authentifizierungs-App festgelegte Zeit mit der Zeit des Administrationsservers synchronisiert wird.

3. **Aktivieren der Zwei-Faktor-Authentifikation für Ihr Benutzerkonto und Anfordern des geheimen Schlüssels für Ihr Benutzerkonto**

   Nachdem Sie die Zwei-Faktor-Authentifikation für Ihr Benutzerkonto aktiviert haben, können Sie die Zwei-Faktor-Authentifikation für alle Benutzer aktivieren.

4. **Die Zwei-Faktor-Authentifikation für alle Benutzer aktivieren**

Benutzer, für welche die Zwei-Faktor-Authentifikation aktiviert ist, müssen diese verwenden, um sich am Administrationsserver anmelden.

5. **Den Namen eines Sicherheitscode-Ausstellers bearbeiten**

   Wenn Sie mehrere Administrationsserver mit ähnlichen Namen haben, müssen Sie möglicherweise die Namen der Sicherheitscode-Aussteller ändern, um verschiedene Administrationsserver besser unterscheiden zu können.

6. **Ausschließen der Benutzerkonten, für die Sie die Zwei-Faktor-Authentifikation nicht aktivieren müssen**

   Bei Bedarf können Sie Benutzerkonten von der Zwei-Faktor-Authentifikation ausschließen. Benutzer mit ausgeschlossenen Benutzerkonten müssen sich nicht mittels Zwei-Faktor-Authentifikation am Administrationsserver anmelden.

Ergebnisse

Nach Abschluss dieses Szenarios:

- Die Zwei-Faktor-Authentifikation ist für Ihr Konto aktiviert.
- Die Zwei-Faktor-Authentifikation ist für alle Benutzerkonten des Administrationsservers aktiviert, mit Ausnahme der Benutzerkonten, die ausgeschlossenen wurden.

Über die Zwei-Faktor-Authentifikation für ein Benutzerkonto

Mit Kaspersky Security Center Linux können die Benutzer von Kaspersky Security Center 14 Web Console eine Zwei-Faktor-Authentifikation verwenden. Wenn die Zwei-Faktor-Authentifikation für Ihr eigenes Benutzerkonto aktiviert ist, müssen Sie bei jeder Anmeldung an der Kaspersky Security Center 14 Web Console den Benutzernamen, das Kennwort und einen zusätzlichen Einmal-Sicherheitscode eingegeben. Um einen Einmal-Sicherheitscode zu erhalten, benötigen Sie eine Authentifizierungs-App auf einem Ihrer Geräte, z. B. auf Ihrem Computer oder mobilen Gerät.

Ein Sicherheitscode besitzt eine Kennung, die als *Aussteller-Name* bezeichnet wird. Der Name des Sicherheitscode-Ausstellers wird als Kennung des Administrationsservers in der Authentifizierungs-App verwendet. Sie können den Namen des Sicherheitscode-Ausstellers ändern. Der Standardwert für den Namen des Sicherheitscode-Ausstellers entspricht dem Namen des Administrationsservers. Der Aussteller-Name wird als Kennung des Administrationsservers in der Authentifizierungs-App verwendet. Wenn Sie den Namen des Sicherheitscode-Ausstellers ändern, müssen Sie einen neuen geheimen Schlüssel ausstellen und an die Authentifizierungs-App übergeben. Ein Sicherheitscode ist einmalig verwendbar und bis zu 90 Sekunden lang gültig (die genaue Zeit kann variieren).

Jeder Benutzer, für den die Zwei-Faktor-Authentifikation aktiviert ist, kann den eigenen geheimen Schlüssel erneut ausstellen. Wenn sich ein Benutzer mit dem neu ausgestellten geheimen Schlüssel authentifiziert und diesen zur Anmeldung verwendet, speichert der Administrationsserver den neuen geheimen Schlüssel für das Benutzerkonto. Wenn ein Benutzer einen ungültigen neuen geheimen Schlüssel eingibt, speichert der Administrationsserver diesen neuen geheimen Schlüssel nicht und erachtet den aktuellen geheimen Schlüssel für die Authentifizierung weiterhin als gültig.

Jede Authentifizierungssoftware, die den Algorithmus für zeitbasierte Einmalkennwörter (Time-based One-time Password – TOTP) unterstützt, ist als Authentifizierungs-App geeignet, z. B. der Google Authenticator. Um den Sicherheitscode zu generieren, müssen Sie die in der Authentifizierungs-App eingestellte Zeit mit der eingestellten Zeit des Administrationsservers synchronisieren.

Eine Authentifizierungs-App generiert den Sicherheitscode wie folgt:

1. Der Administrationsserver erstellt einen speziellen geheimen Schlüssel sowie einen QR-Code.
2. Sie übergeben den erstellten geheimen Schlüssel oder QR-Code an die Authentifizierungs-App.
3. Die Authentifizierungs-App generiert einen Einmal-Sicherheitscode, den Sie an das Authentifizierungsfenster des Administrationsservers übergeben.

Es wird dringend empfohlen, eine Authentifizierungs-App auf mehreren mobilen Geräten zu installieren. Speichern Sie den geheimen Schlüssel (oder den QR-Code) ab und bewahren Sie ihn an einem sicheren Ort auf. Auf diese Weise können Sie den Zugriff auf die Kaspersky Security Center 14 Web Console wiederherstellen, falls Sie den Zugriff auf Ihr mobiles Gerät verlieren.

Um die Verwendung von Kaspersky Security Center abzusichern, können Sie die Zwei-Faktor-Authentifikation für Ihr eigenes Konto und die Zwei-Faktor-Authentifikation für alle Benutzer aktivieren.

Sie können Benutzerkonten von der Zwei-Faktor-Authentifikation ausschließen. Dies kann für Dienstkonten erforderlich sein, die den zur Authentifizierung notwendigen Sicherheitscode nicht empfangen können.

Die Zwei-Faktor-Authentifikation funktioniert entsprechend den folgenden Regeln:

- Nur ein Benutzerkonto, das die Berechtigung "Objekt-ACL ändern" im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** besitzt, kann die Zwei-Faktor-Authentifikation für alle Benutzer aktivieren.
- Nur ein Benutzer, der die Zwei-Faktor-Authentifikation für das eigene Konto aktiviert hat, kann die Option zur Zwei-Faktor-Authentifikation für alle Benutzer aktivieren.
- Nur ein Benutzer, der die Zwei-Faktor-Authentifikation für das eigene Konto aktiviert hat, kann andere Benutzerkonten von der Liste mit Benutzern, für welche die Zwei-Faktor-Authentifikation aktiviert ist, ausschließen.
- Ein Benutzer kann die Zwei-Faktor-Authentifikation nur für sein eigenes Konto aktivieren.
- Ein Benutzerkonto, das die Berechtigung "Objekt-ACLs ändern" im Funktionsbereich **Allgemeine Funktionen: Benutzerrechte** besitzt und das an der Kaspersky Security Center 14 Web Console mittels Zwei-Faktor-Authentifikation angemeldet ist, kann die Zwei-Faktor-Authentifikation in folgenden Fällen für andere Benutzer deaktivieren: 1) Für jeden anderen Benutzer nur dann, wenn die Zwei-Faktor-Authentifikation für alle Benutzer deaktiviert ist. 2) Für einen Benutzer, der von der Liste der für alle Benutzer aktivierten Zwei-Faktor-Authentifikation ausgeschlossen ist.
- Jeder Benutzer, der sich mithilfe der Zwei-Faktor-Authentifikation an der Kaspersky Security Center 14 Web Console angemeldet hat, kann den eigenen geheimen Schlüssel erneut ausstellen.
- Sie können die Option zur Zwei-Faktor-Authentifikation aller Benutzer für den Administrationsserver aktivieren, mit dem Sie gerade arbeiten. Wenn Sie diese Option auf dem Administrationsserver aktivieren, wird Sie diese Option auch für die Benutzerkonten der virtuellen Administrationsserver aktiviert. Sie aktivieren jedoch nicht die Zwei-Faktor-Authentifikation für die Benutzerkonten der sekundären Administrationsserver.

Wenn für ein Benutzerkonto auf dem Kaspersky Security Center Administrationsserver ab Version 13 eine Zwei-Faktor-Authentifikation aktiviert ist, kann sich der Benutzer nicht an der Kaspersky Security Center Web Console in den Versionen 12, 12.1 oder 12.2 anmelden.

Die Zwei-Faktor-Authentifikation für Ihr eigenes Benutzerkonto aktivieren

Sie können die Zwei-Faktor-Authentifikation nur für Ihr eigenes Konto aktivieren.

Bevor Sie beginnen, die Zwei-Faktor-Authentifikation für Ihr Konto zu aktivieren, müssen Sie unbedingt sicherstellen, dass auf Ihrem mobilen Gerät eine Authenticator-App installiert ist. Stellen Sie sicher, dass die in der Authentifizierungs-App festgelegte Zeit mit der Zeit auf dem Gerät, auf dem der Administrationsserver installiert ist, synchronisiert wird.

Um die Zwei-Faktor-Authentifikation für ein Benutzerkonto zu aktivieren:

1. Gehen Sie zu **BENUTZER UND ROLLEN** → **BENUTZER**.
2. Klicken Sie auf den Namen Ihres Benutzerkontos.
3. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Schutz des Benutzerkontos**.
4. Auf der Registerkarte **Schutz des Benutzerkontos**:
   - Wählen Sie die Option **Benutzername, Kennwort und Sicherheitscode abfragen (Zwei-Faktor-Authentifikation)**, wenn Sie die Zwei-Faktor-Authentifikation für ein Benutzerkonto aktivieren möchten:
     - Geben Sie im angezeigten Fenster zur Zwei-Faktor-Authentifikation entweder den geheimen Schlüssel in die Authentifizierungs-App ein oder scannen Sie den QR-Code und fordern Sie so einen Einmal-Sicherheitscode an.

       Sie können den geheimen Schlüssel manuell in der Authentifizierungs-App angeben oder den QR-Code mit Ihrem mobilen Gerät scannen.

     - Geben Sie im Fenster zur Zwei-Faktor-Authentifikation den Sicherheitscode an, der von der Authentifizierungs-App generiert wurde, und klicken Sie dann auf **Überprüfen und anwenden**.
5. Klicken Sie auf **Speichern**.

Die Zwei-Faktor-Authentifikation ist für Ihr Konto aktiviert.

Die Zwei-Faktor-Authentifikation für alle Benutzer aktivieren

Sie können die Zwei-Faktor-Authentifikation für alle Benutzer des Administrationsservers aktivieren, wenn Ihr Benutzerkonto über die Berechtigung "Objekt-ACL ändern" im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** verfügt und wenn Sie sich mittels Zwei-Faktor-Authentifikation authentifiziert haben. Wenn Sie die zwei-Faktor-Authentifikation für Ihr Benutzerkonto nicht aktiviert haben, bevor Sie es für alle Benutzer aktivieren, öffnet die Anwendung das Fenster zum Aktivieren der Zwei-Faktor-Authentifikation für Ihr eigenes Konto.

So aktivieren Sie die Zwei-Faktor-Authentifikation für alle Benutzer:

1. Klicken Sie im Hauptfenster der Anwendung neben dem Namen des benötigten Administrationsservers auf das Symbol **Einstellungen** ( ).

Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Schalten Sie in der Registerkarte **Sicherheit für die Authentifizierung** des Eigenschaftenfensters den Umschalter für die **Zwei-Faktor-Authentifikation für alle Benutzer** in die Position "aktiviert".

Die Zwei-Faktor-Authentifikation ist für alle Benutzer aktiviert. Von nun an müssen Benutzer des Administrationsservers, einschließlich der Benutzer, die nach der Aktivierung der Zwei-Faktor-Authentifikation hinzugefügt wurden, die Zwei-Faktor-Authentifikation für ihre Konten konfigurieren. Ausgenommen sind Benutzer, die von der Zwei-Faktor-Authentifikation ausgeschlossen sind.

Die Zwei-Faktor-Authentifikation für ein Benutzerkonto deaktivieren

Sie können die Zwei-Faktor-Authentifikation für Ihr eigenes Benutzerkonto sowie für das Konto eines anderen Benutzers deaktivieren.

Sie können die Zwei-Faktor-Authentifikation für das Konto eines anderen Benutzers nur dann deaktivieren, wenn Ihr Benutzerkonto die Berechtigung "Objekt-ACL ändern" im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** besitzt.

Um die Zwei-Faktor-Authentifikation für ein Benutzerkonto zu deaktivieren:

1. Gehen Sie zu **BENUTZER UND ROLLEN** → **BENUTZER**.
2. Klicken Sie auf den Namen des internen Benutzerkontos, für das Sie die Zwei-Faktor-Authentifikation deaktivieren möchten. Dies kann Ihr eigenes Benutzerkonto oder das Konto eines anderen Benutzers sein.
3. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Schutz des Benutzerkontos**.
4. Wählen Sie auf der Registerkarte **Schutz des Benutzerkontos** die Option **Nur Benutzername und Kennwort abfragen**, wenn Sie die Zwei-Faktor-Authentifikation für ein Benutzerkonto deaktivieren möchten.
5. Klicken Sie auf **Speichern**.

Die Zwei-Faktor-Authentifikation ist jetzt für das Benutzerkonto deaktiviert.

Die Zwei-Faktor-Authentifikation für alle Benutzer deaktivieren

Sie können die Zwei-Faktor-Authentifikation für alle Benutzer deaktivieren, wenn die Zwei-Faktor-Authentifikation für Ihr Benutzerkonto aktiviert ist und Ihr Konto die Berechtigung "Objekt-ACL ändern" im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** hat. Wenn die Zwei-Faktor-Authentifikation für Ihr Benutzerkonto nicht aktiviert ist, müssen Sie die Zwei-Faktor-Authentifikation für Ihr Konto aktivieren, bevor Sie sie für alle Benutzer deaktivieren.

So deaktivieren Sie die Zwei-Faktor-Authentifikation für alle Benutzer:

1. Klicken Sie im Hauptfenster der Anwendung neben dem Namen des benötigten Administrationsservers auf das Symbol **Einstellungen** ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Schalten Sie in der Registerkarte **Sicherheit für die Authentifizierung** des Eigenschaftenfensters den Umschalter für die **Zwei-Faktor-Authentifikation für alle Benutzer** in die Position "deaktiviert".

3. Geben Sie die Anmeldedaten Ihres Benutzerkontos im Authentifizierungsfenster ein.

Die Zwei-Faktor-Authentifikation ist für alle Benutzer deaktiviert.

Benutzerkonten von der Zwei-Faktor-Authentifikation ausschließen

Sie können Benutzerkonten von der Zwei-Faktor-Authentifikation ausschließen, wenn Sie die Berechtigung "Objekt-ACL ändern" im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** haben.

Wenn ein Benutzerkonto von der Liste der Zwei-Faktor-Authentifikation für alle Benutzer ausgeschlossen ist, muss dieser Benutzer die Zwei-Faktor-Authentifikation nicht verwenden.

> Das Ausschließen von Benutzerkonten von der Zwei-Faktor-Authentifikation kann für Dienstkonten erforderlich sein, die den Sicherheitscode während der Authentifikation nicht übergeben können.

Wenn Sie bestimmte Benutzerkonten von der Zwei-Faktor-Authentifikation ausschließen möchten:

1. Klicken Sie im Hauptfenster der Anwendung neben dem Namen des benötigten Administrationsservers auf das Symbol **Einstellungen** ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Klicken Sie auf der Registerkarte **Sicherheit für die Authentifizierung** des Eigenschaftenfensters, in der Tabelle mit den Ausschlüssen aus der Zwei-Faktor-Authentifikation, auf die Schaltfläche **Hinzufügen**.

3. Führen Sie in dem neuen Fenster folgende Schritte aus:

   a. Wählen Sie die Benutzerkonten aus, die Sie ausschließen möchten.

   b. Klicken Sie auf die Schaltfläche **Uhrzeit der Verschlüsselung**.

Die ausgewählten Benutzerkonten werden von der Zwei-Faktor-Authentifikation ausgeschlossen.

Neuen geheimen Schlüssel generieren

Sie können nur dann einen neuen geheimen Schlüssel für die Zwei-Faktor-Authentifikation Ihres Benutzerkontos generieren, wenn Sie sich mithilfe der Zwei-Faktor-Authentifikation autorisiert haben.

Um einen neuen geheimen Schlüssel für ein Benutzerkonto zu generieren:

1. Gehen Sie zu **BENUTZER UND ROLLEN** → **BENUTZER**.

2. Klicken Sie auf den Namen des Benutzerkontos, für das Sie einen neuen geheimen Schlüssel für die Zwei-Faktor-Authentifikation generieren möchten.

3. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Schutz des Benutzerkontos**.

4. Klicken Sie auf der Registerkarte **Schutz des Benutzerkontos** auf den Link **Neuen geheimen Schlüssel generieren**.

5. Geben Sie im angezeigten Fenster zur Zwei-Faktor-Authentifikation einen neuen Sicherheitsschlüssel an, der von der Authentifizierungs-App generiert wird.

6. Klicken Sie auf die Schaltfläche **Überprüfen und anwenden**.

Für den Benutzer wird ein neuer geheimer Schlüssel generiert.

Wenn Sie Ihr Mobilgerät verlieren, können Sie auf einem anderen Mobilgerät eine Authentifizierungs-App installieren und einen neuen geheimen Schlüssel generieren, um den Zugriff auf die Kaspersky Security Center 14 Web Console wiederherzustellen.

Den Namen eines Sicherheitscode-Ausstellers bearbeiten

Möglicherweise haben Sie mehrere Identifikatoren (auch "Aussteller" genannt) für verschiedene Administrationsserver. Sie können den Namen eines Sicherheitscode-Ausstellers ändern, beispielsweise wenn der Administrationsserver bereits einen ähnlichen Namen eines Sicherheitscode-Ausstellers für einen anderen Administrationsserver verwendet. Standardmäßig entspricht der Name eines Sicherheitscode-Ausstellers dem Namen des Administrationsservers.

Nachdem Sie den Namen des Sicherheitscode-Ausstellers geändert haben, müssen Sie einen neuen geheimen Schlüssel ausstellen und an die Authentifizierungs-App übergeben.

So geben Sie einen neuen Namen des Sicherheitscode-Ausstellers an:

1. Klicken Sie im Hauptfenster der Anwendung neben dem Namen des benötigten Administrationsservers auf das Symbol **Einstellungen** ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Schutz des Benutzerkontos**.

3. Klicken Sie auf der Registerkarte **Schutz des Benutzerkontos** auf den Link **Bearbeiten**.

   Der Abschnitt **Aussteller des Sicherheitscodes ändern** wird geöffnet.

4. Geben Sie einen neuen Namen für den Sicherheitscode-Aussteller an.

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

Für den Administrationsserver wird jetzt ein neuer Name des Sicherheitscode-Ausstellers angezeigt.

Ändern der Anzahl der zulässigen Kennworteingabeversuche

Die Benutzer von Kaspersky Security Center Linux haben nur eine begrenzte Anzahl von Eingabeversuchen mit ungültigen Kennwörtern. Wenn das Limit erreicht ist, wird das Benutzerkonto für eine Stunde gesperrt.

Standardmäßig liegt die maximale Anzahl zulässiger Versuche zur Eingabe eines Kennworts bei 10. Sie können die Anzahl der zulässigen Kennworteingabeversuche ändern (siehe Beschreibung in diesem Abschnitt).

So ändern Sie die Anzahl der zulässigen Kennworteingabeversuche:

1. Führen Sie auf dem Administrationsserver-Gerät eine Linux-Befehlszeile aus.
2. Führen Sie für das Dienstprogramm klscflag den folgenden Befehl aus:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

   Dabei steht N für die Anzahl der zulässigen Kennworteingabeversuche.
3. Um die Änderungen zu übernehmen, starten Sie den Administrationsserver-Dienst neu.

Die maximale Anzahl der Eingabeversuche für das Kennwort wird geändert.

DBMS-Anmeldedaten ändern

In einigen Fällen müssen Sie möglicherweise die DBMS-Anmeldedaten ändern, beispielsweise um aus Sicherheitsgründen eine Rotation der Anmeldedaten auszuführen.

Um die DBMS-Anmeldedaten in einer Linux-Umgebung mithilfe des Dienstprogramms klsrvconfig zu ändern:

1. Starten Sie eine Linux-Befehlszeile.
2. Geben Sie im angezeigten Befehlszeilenfenster das Dienstprogramm klsrvconfig an:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```
3. Geben Sie einen neuen Kontonamen an. Sie sollten die Anmeldedaten eines Benutzerkontos angeben, das im DBMS vorhanden ist.
4. Geben Sie ein neues Kennwort ein.
5. Geben Sie das neue Kennwort erneut zur Bestätigung ein.

Die DBMS-Anmeldeinformationen werden geändert.

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 oberen Bereich des Bildschirms auf das Symbol **Einstellungen** ( ) neben dem Namen des primären Administrationsservers.
2. Wechseln Sie auf der nächsten Seite auf die Registerkarte **Administrationsserver**.
3. Wählen Sie in der Administrationsgruppe, aus der Sie den sekundären Administrationsserver löschen möchten, den entsprechenden Server aus.
4. Klicken Sie in der Menüleiste auf **Löschen**.
5. Klicken Sie im nächsten Fenster auf **OK**, um das Löschen des sekundären Administrationsservers zu bestätigen.

Der ehemalige primäre Administrationsserver und der ehemalige sekundäre Administrationsserver sind nun unabhängig voneinander. Die Hierarchie ist nicht mehr vorhanden.

Konfiguration der Schnittstelle

Sie können die Benutzeroberfläche der Kaspersky Security Center 14 Web Console so konfigurieren, dass Abschnitte und Elemente der Benutzeroberfläche abhängig von den verwendeten Funktionen ein- und ausgeblendet werden.

So konfigurieren Sie die Benutzeroberfläche der Kaspersky Security Center 14 Web Console gemäß den derzeit verwendeten Funktionen:

1. Klicken Sie im Hauptfenster des Programms auf das Menü des Benutzerkontos.
2. Wählen Sie im Dropdown-Menü den Punkt **Einstellungen der Benutzeroberfläche** aus.
3. Aktivieren oder deaktivieren Sie im folgenden Fenster **Einstellungen der Benutzeroberfläche** die erforderlichen Optionen.
4. Klicken Sie auf **Speichern**.

Danach werden die Abschnitte des Hauptmenüs in der Konsole entsprechend den aktivierten Optionen angezeigt. Wenn Sie beispielsweise **Alarme von EDR anzeigen** aktivieren, wird der Abschnitt **ÜBERWACHUNG UND BERICHTERSTATTUNG → ALARME** im Hauptmenü angezeigt.

Geräte im Netzwerk finden

In diesem Abschnitt wird die Suche und Entdeckung von Geräten im Netzwerk beschrieben.

Kaspersky Security Center ermöglicht eine Suche der Geräte auf der Grundlage der angegebenen Kriterien. Sie können Suchergebnisse in einer Textdatei speichern.

Mit der Such- und Ermittlungsfunktion können folgende Geräte gefunden werden:

- Verwaltete Geräte der Administrationsgruppen des Kaspersky Security Center Administrationsservers und seiner sekundären Administrationsserver.
- Nicht zugeordnete Geräte, die vom Kaspersky Security Center Administrationsservers und seiner sekundären Administrationsserver verwaltet werden.

Szenario: Suche nach Netzwerkgeräten

Die Gerätesuche muss vor der Installation 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 die bereits erkannten Geräte sich noch im Netzwerk befinden.

Das Erkennen von Geräten im Netzwerk erfolgt in mehreren Etappen:

1. **Erstmalige Gerätesuche**

   Führen Sie nach Abschluss des Schnellstartassistenten die Gerätesuche manuell aus.

2. **Zukünftige Abfragen konfigurieren**

   Stellen Sie sicher, dass IP-Bereiche durchsuchen aktiviert ist und dass der Abfragezeitplan die Anforderungen Ihres Unternehmens erfüllt. Verwenden Sie bei der Konfiguration des Abfragezeitplans die Empfehlungen zur Häufigkeit der Netzwerkabfrage.

   Sie können auch Zeroconf-Abfragen aktivieren, wenn Ihr Netzwerk IPv6-Geräte enthält.

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 zur Gruppe **Verwaltete Geräte** verschoben werden. Darüber hinaus können Sie Aufbewahrungsregeln einrichten.

   Wenn Sie diese Etappe der Regelerstellung überspringen, werden alle neu entdeckten Geräte zur Gruppe **Nicht zugeordnete Geräte** hinzugefügt und bleiben 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.

Ergebnisse

Der Abschluss des Szenarios bringt folgende Ergebnisse mit sich:

- Der Kaspersky Security Center Linux Administrationsserver findet die Geräte im Netzwerk und stellt Ihnen Informationen zu diesen Geräten zur Verfügung.

- Zukünftige Abfragen werden eingerichtet und nach einem festgelegten Zeitplan ausgeführt.

Neu entdeckte Geräte werden gemäß den konfigurierten Regeln bestimmten Gruppen zugewiesen. (Falls keine Regeln erstellt wurden, bleiben die Geräte in der Gruppe **Nicht zugeordnete Geräte**).

IP-Bereiche abfragen

Kaspersky Security Center versucht für jede IPv4-Adresse aus dem festgelegten Bereich eine umgekehrte Namensauflösung zu einem DNS-Namen mithilfe von Standard-DNS-Abfragen durchzuführen. Wenn dieser Vorgang erfolgreich ist, sendet der Server einen `ICMP ECHO REQUEST` (entspricht einem ping-Befehl) an den empfangenen Namen. Wenn das Gerät antwortet, werden die Informationen darüber zur Kaspersky Security Center-Datenbank hinzugefügt. Die umgekehrte Namensauflösung ist erforderlich, um Netzwerkgeräte auszuschließen, die über eine IP-Adresse verfügen können, aber keine Computer sind (Netzwerkdrucker, Router usw.).

Dieses Abfrageverfahren benötigt einen korrekt konfigurierten DNS-Dienst. Dieser muss über eine Reverse-Lookupzone verfügen. Wenn diese Zone nicht konfiguriert ist, ergibt die IP-Subnetzabfrage keine Ergebnisse.

Ursprünglich erhält Kaspersky Security Center IP-Bereiche für die Abfrage aus den Netzwerk-Einstellungen des Geräts, auf dem es installiert ist. Wenn die Geräteadresse 192.168.0.1 lautet und die Subnetzmaske 255.255.255.0 ist, fügt Kaspersky Security Center das Netzwerk 192.168.0.0/24 automatisch zur Liste der Abfrageadressen hinzu. Kaspersky Security Center fragt alle Adressen von 192.168.0.1 bis 192.168.0.254 ab.

Wenn nur die IP-Bereichsabfrage aktiviert ist, erkennt Kaspersky Security Center nur Geräte mit IPv4-Adressen. Wenn Ihr Netzwerk IPv6-Geräte enthält, aktivieren Sie die Zeroconf-Abfrage von Geräten.

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. Gehen Sie zu **GERÄTESUCHE UND SOFTWAREVERTEILUNG → ENTDECKUNG → IP-BEREICHE**.
2. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Eigenschaftenfenster der IP-Abfrage wird geöffnet.
3. Aktivieren oder deaktivieren Sie die IP-Abfrage mit dem Schalter **Abfrage erlauben**.
4. Passen Sie den Abfragezeitplan an. Standardmäßig wird die IP-Abfrage alle 420 Minuten (sieben Stunden) ausgeführt.

   Achten Sie bei der Angabe des Abfrageintervalls darauf, dass diese Angabe den Wert der Lebensdauer der IP-Adresse nicht übersteigt. Wird eine IP-Adresse nicht innerhalb ihrer Lebensdauer durch eine Abfrage verifiziert, wird sie automatisch aus den Abfrageergebnissen entfernt. Standardmäßig beträgt die Lebensdauer der Abfrageergebnisse 24 Stunden, da dynamische IP-Adressen (mithilfe des DHCP-Protokolls (Dynamic Host Configuration Protocol) zugewiesen) alle 24 Stunden geändert werden.

   Varianten für den Zeitplan der Abfrage:

   - **Alle n Tage**

     Die Abfrage wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Tagen ausgeführt.

     Standardmäßig wird die Abfrage ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

- **Alle n Minuten**

  Die Abfrage wird ab der angegebenen Uhrzeit regelmäßig im angegebenen Intervall in Minuten ausgeführt.

- **Nach Wochentagen**

  Die Abfrage wird regelmäßig an den festgelegten Wochentagen und zur festgelegten Uhrzeit ausgeführt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Abfrage wird regelmäßig an den festgelegten Tagen des Monats und zur festgelegten Uhrzeit ausgeführt.

- **Übersprungene Aufgaben starten**

  Wenn der Administrationsserver während der für die Abfrage geplanten Zeit abgeschaltet oder nicht verfügbar ist, kann der Administrationsserver die Abfrage entweder sofort nachdem er eingeschaltet wurde starten, oder auf die nächste planmäßige Durchführung warten.

  Wenn diese Option aktiviert ist, startet der Administrationsserver die Abfrage sofort nachdem er eingeschaltet wurde.

  Wenn diese Option deaktiviert ist, wartet der Administrationsserver auf den nächsten Zeitpunkt, für den die Abfrage geplant ist.

  Diese Option ist standardmäßig deaktiviert.

5. Klicken Sie auf die Schaltfläche **Speichern**.

Die Eigenschaften werden gespeichert und auf alle IP-Bereiche angewendet.

Abfrage manuell ausführen

Um die Abfrage sofort auszuführen,

klicken Sie auf die Schaltfläche **Abfrage starten**.

IP-Bereich hinzufügen und bearbeiten

Ursprünglich erhält Kaspersky Security Center IP-Bereiche für die Abfrage aus den Netzwerk-Einstellungen des Geräts, auf dem es installiert ist. Wenn die Geräteadresse 192.168.0.1 lautet und die Subnetzmaske 255.255.255.0 ist, fügt Kaspersky Security Center das Netzwerk 192.168.0.0/24 automatisch zur Liste der Abfrageadressen hinzu. Kaspersky Security Center fragt alle Adressen von 192.168.0.1 bis 192.168.0.254 ab. Sie können die automatisch festgelegten IP-Bereiche bearbeiten oder eigene IP-Bereiche hinzufügen.

Bereiche können nur für IPv4-Adressen erstellt werden. Wenn Sie die Zeroconf-Abfrage aktivieren, wird Kaspersky Security Center das gesamte Netzwerk abfragen.

Um einen neuen IP-Bereich hinzuzufügen, gehen Sie wie folgt vor:

1. Gehen Sie zu **GERÄTESUCHE UND SOFTWAREVERTEILUNG → ENTDECKUNG → IP-BEREICHE**.
2. Klicken Sie auf **Hinzufügen**, um den neuen IP-Bereich hinzuzufügen.
3. Passen Sie im nächsten Fenster folgende Einstellungen an:
   - **Name des IP-Bereichs**

     Der Name des IP-Bereichs. Sie können den IP-Bereich selbst als Namen angeben, z. B. "192.168.0.0/24".

   - **IP-Intervall oder Subnetzadresse und Maske**

     Legen Sie den IP-Bereich fest, indem Sie entweder die erste und letzte IP-Adresse oder die Subnetzadresse und Subnetzmaske angeben. Sie können auch einen der bereits vorhandenen IP-Bereiche auswählen, indem Sie auf **Durchsuchen** klicken.

   - **Gültigkeitsdauer der IP-Adresse (Stunden)**

     Stellen Sie bei Angabe dieser Einstellung sicher, dass die Lebensdauer das im Abfragezeitplan festgelegte Abfrageintervall übersteigt. Wird eine IP-Adresse nicht innerhalb ihrer Lebensdauer durch eine Abfrage verifiziert, wird sie automatisch aus den Abfrageergebnissen entfernt. Standardmäßig beträgt die Lebensdauer der Abfrageergebnisse 24 Stunden, da dynamische IP-Adressen (mithilfe des Protokolls für dynamische Konfiguration von Hosts – DHCP zugewiesen) alle 24 Stunden geändert werden.

4. Wählen Sie **Abfrage des IP-Bereichs zulassen**, wenn Sie das hinzugefügte Subnetz oder den Bereich abfragen möchten. Andernfalls wird das hinzugefügte Subnetz oder der Bereich nicht abgefragt.
5. Klicken Sie auf die Schaltfläche **Speichern**.

Der neue IP-Bereich wird zur Liste mit IP-Bereichen hinzugefügt.

Sie können jeden IP-Bereich separat durchsuchen, indem Sie auf **Abfrage starten** klicken. Nach Abschluss der Abfrage können Sie über die Schaltfläche **Geräte** eine Liste mit entdeckten Geräten anzeigen. Standardmäßig beträgt die Lebensdauer der Abfrageergebnisse 24 Stunden und entspricht der festgelegten Lebensdauer der IP-Adresse.

Um eine neues Subnetz zu einem vorhandenen IP-Bereich hinzuzufügen, gehen Sie wie folgt vor:

1. Gehen Sie zu **GERÄTESUCHE UND SOFTWAREVERTEILUNG → ENTDECKUNG → IP-BEREICHE**.
2. Klicken Sie auf den Namen des IP-Bereichs, zu dem Sie ein Subnetz hinzufügen möchten.
3. Klicken Sie im folgenden Fenster auf **Hinzufügen**.
4. Geben Sie ein Subnetz an, indem Sie entweder dessen Adresse und Maske oder die erste und letzte IP-Adresse im IP-Bereich verwenden. Sie können auch ein vorhandenes Subnetz hinzufügen, indem Sie auf **Durchsuchen** klicken.
5. Klicken Sie auf die Schaltfläche **Speichern**.

   Das neue Subnetz wird zum IP-Bereich hinzugefügt.

6. Klicken Sie auf die Schaltfläche **Speichern**.

Die neuen Einstellungen des IP-Bereichs werden gespeichert.

Sie können beliebig viele Subnetze hinzufügen. Benannte IP-Bereiche dürfen sich nicht überlappen, aber für unbenannte Subnetze innerhalb eines IP-Bereichs gilt keine derartige Beschränkung. Sie können die Abfrage für jeden IP-Bereich unabhängig aktivieren und deaktivieren.

Zeroconf-Abfrage

Diese Art der Abfrage wird nur von Linux-basierten Verteilungspunkten unterstützt.

Kaspersky Security Center kann Netzwerke abfragen, die Geräte mit IPv6-Adressen enthalten. In diesem Fall werden keine IP-Bereiche angegeben, und Kaspersky Security Center fragt das gesamte Netzwerk unter Verwendung von Zero-configuration Networking (auch als *Zeroconf* bezeichnet) ab. Um mit der Verwendung von Zeroconf zu beginnen, müssen Sie das Dienstprogramm avahi-browse auf dem Linux-Gerät installieren, das Netzwerke abfragt, also auf dem Administrationsserver oder einem Verteilungspunkt.

So aktivieren Sie die Zeroconf-Abfrage:

1. Gehen Sie zu **GERÄTESUCHE UND SOFTWAREVERTEILUNG → ENTDECKUNG → IP-BEREICHE**.
2. Klicken Sie auf die Schaltfläche **Eigenschaften**.
3. Aktivieren Sie im angezeigten Fenster die Umschaltfläche **Zeroconf zum Abfragen von IPv6-Netzwerken verwenden**.

Danach beginnt Kaspersky Security Center das Netzwerk abzufragen. In diesem Fall werden die angegeben IP-Bereiche ignoriert.

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 erlaubt, 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 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. Beispielsweise können Sie eine Regel konfigurieren, nach der allen Geräten, die unter dem Betriebssystem CentOS laufen, das Tag `[CentOS]` zugewiesen wird. Dieses Tag kann anschließend beim Erstellen einer Geräteauswahl verwendet werden, die Sie dabei unterstützt, alle CentOS-Geräte auszuwählen und diesen 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 Optionsfeld neben dem Geräte-Tag, 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.

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 **Uhrzeit der Verschlüsselung**, 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. Zeigen Sie die zugewiesenen Tags von dem Gerät an, von welchem Sie ein Tag entfernen möchten.
2. Aktivieren Sie das Kontrollkästchen neben dem Tag, das Sie entfernen möchten.
3. Klicken Sie auf die Schaltfläche **Tag-Zuweisen aufheben**.
4. 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.

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** und klicken Sie 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 **Uhrzeit der Verschlüsselung**.
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 DNS-Name des Gerätes oder Zugehörigkeit des Gerätes zu einem IP-Subnetz).
   - **Programme** – Vorhandensein des Administrationsagenten auf dem Gerät, Typ, Version und Betriebssystemarchitektur.
   - **Virtuelle Maschinen** – Das Gerät gehört zu einem speziellen Typ für virtuelle Maschinen.
   - **Programm-Registry** – Vorhandensein von Programmen verschiedener Hersteller auf dem Gerät.
7. Klicken Sie auf die Schaltfläche **Uhrzeit der Verschlüsselung**, 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, zu der ein solches Gerät gehört.

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.

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 Linux ermöglicht das Zuweisen von Tags an 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 einer Geräteauswahl 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 **Uhrzeit der Verschlüsselung**, 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 **Uhrzeit der Verschlüsselung**, 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 sie 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 **Uhrzeit der Verschlüsselung**.

Das Programm-Tag wird gelöscht. Das gelöschte Tag wird automatisch von allen Programmen entfernt, denen es zugewiesen war.

Bereitstellung von Kaspersky-Programmen

Dieser Abschnitt beschreibt die Bereitstellung von Kaspersky-Programmen auf Client-Geräten in Ihrem Unternehmen mithilfe von Kaspersky Security Center 14 Web Console.

Szenario: Bereitstellung von Kaspersky-Programmen

Dieses Szenario erklärt, wie Kaspersky-Anwendungen über Kaspersky Security Center 14 Web Console verteilt werden. Sie können den Schnellstartassistenten und den Assistenten für die Bereitstellung des Schutzes verwenden oder alle erforderlichen Schritte manuell ausführen.

Die Bereitstellung von Kaspersky-Programmen erfolgt schrittweise:

1. **Download des Verwaltungs-Web-Plug-ins für das Programm**

   Laden Sie das Verwaltungs-Web-Plug-in für Kaspersky Endpoint Security für Linux von der Kaspersky-Website herunter und fügen Sie das Plug-in dann zu Kaspersky Security Center 14 Web Console hinzu.

2. **Download und Erstellen des Installationspakets für den Administrationsagenten**

   Laden Sie das Distributionspaket des Administrationsagenten von der Kaspersky-Website herunter und erstellen Sie dann ein Installationspaket für den Administrationsagenten.

   Zur lokalen Installation des Administrationsagenten können Sie das heruntergeladene Distributionspaket verwenden. Befolgen Sie dazu die Anweisungen in der Dokumentation zu Kaspersky Endpoint Security für Linux.

3. **Download und Erstellen des Installationspakets für Kaspersky Endpoint Security für Linux**

   Laden Sie das Distributionspaket von Kaspersky Endpoint Security für Linux von der Kaspersky-Website herunter und erstellen Sie dann ein Installationspaket für Kaspersky Endpoint Security für Linux.

4. **Erstellen von autonomen Installationspaketen (optional)**

   Wenn die Installation von Kaspersky-Anwendungen mithilfe von Kaspersky Security Center Linux auf bestimmten Geräten nicht möglich ist (z. B. auf Geräten von Remote-Mitarbeitern), können Sie autonome Installationspakete für Anwendungen erstellen. Wenn Sie autonome Pakete für die Installation von Kaspersky-Programmen verwenden, können Sie die Schritte 5 und 6 überspringen.

5. **Erstellen, Konfigurieren und Ausführen der Remote-Installationsaufgabe**

   Dieser Schritt ist Teil des Assistenten für die Bereitstellung des Schutzes. Wenn Sie den Assistenten für die Bereitstellung des Schutzes nicht ausführen möchten, müssen Sie diese Aufgabe manuell erstellen und konfigurieren.

   Manuell können Sie mehrere Remote-Installationsaufgaben für verschiedene Administrationsgruppen oder unterschiedliche Geräteauswahlen erstellen. Sie können in diesen Aufgaben verschiedene Versionen eines Programms bereitstellen.

   Stellen Sie sicher, dass alle Geräte in Ihrem Netzwerk erkannt wurden. Starten Sie dann die Aufgabe (Aufgaben) zur Remote-Installation.

   > Wenn Sie den Administrationsagenten auf Geräten mit dem Betriebssystem SUSE Linux Enterprise Server 15 installieren möchten, sollten Sie zunächst das Paket insserv-compat installieren, um den Administrationsagenten konfigurieren.

6. **Erstellen und Konfigurieren von Aufgaben**

Die *Update*-Aufgabe von Kaspersky Endpoint Security für Linux muss konfiguriert werden.

Dieser Schritt ist Teil des Schnellstartassistenten: Die Aufgabe wird automatisch mit den Standardeinstellungen erstellt und konfiguriert. Wenn Sie den Assistenten nicht ausgeführt haben, müssen Sie diese Aufgabe manuell erstellen und auch manuell konfigurieren. Wenn Sie den Schnellstartassistenten verwenden, stellen Sie sicher, dass der Zeitplan für die Aufgabe Ihren Anforderungen entspricht. (Standardmäßig ist der geplante Start für die Aufgabe auf **Manuell** eingestellt; möglicherweise möchten Sie eine andere Option auswählen.)

7. **Richtlinien anlegen**

   Erstellen Sie die Richtlinie für Kaspersky Endpoint Security für Linux entweder manuell oder über den Schnellstartassistenten. Sie können die Standardeinstellungen der Richtlinie verwenden. Sie können jedoch die Standardeinstellungen der Richtlinie jederzeit gemäß Ihren Anforderungen ändern.

8. **Untersuchung der Ergebnisse**

   Stellen Sie sicher, dass die Softwareverteilung erfolgreich beendet wurde, das heißt: Jedes Programm besitzt Richtlinien und Aufgaben und diese Programme sind auf den verwalteten Geräten installiert.

Ergebnisse

Der Abschluss des Szenarios bringt folgende Ergebnisse mit sich:

- Es werden alle erforderlichen Richtlinien und Aufgaben für die ausgewählten Programme erstellt.
- Die Zeitpläne der Aufgaben werden gemäß Ihren Anforderungen angepasst.
- Die ausgewählten Programme wurden auf den ausgewählten Client-Geräten verteilt oder werden nach Zeitplan verteilt.

Verwaltungs-Plug-ins für Kaspersky-Programme hinzufügen

Um ein Kaspersky-Programm wie beispielsweise Kaspersky Endpoint Security für Linux zu bereitzustellen, müssen Sie das entsprechende Verwaltungs-Web-Plug-in herunterladen und hinzufügen.

Um ein Verwaltungs-Web-Plug-in für ein Kaspersky-Programm herunterzuladen und zu installieren:

1. Laden Sie das Verwaltungs-Web-Plug-in für Kaspersky Endpoint Security für Linux von der Kaspersky-Website herunter.
2. Öffnen Sie Kaspersky Security Center 14 Web Console.
3. Wählen Sie in der Dropdown-Liste **Konsolen-Einstellungen** die Option **Web-Plug-ins**.

   Eine Liste der verfügbaren Verwaltungs-Plug-ins wird angezeigt.
4. Klicken Sie auf die Schaltfläche **Aus Datei hinzufügen**.

   Das Fenster **Aus Datei hinzufügen** wird angezeigt.
5. Klicken Sie auf die Schaltfläche **ZIP-Datei hochladen**.
6. Geben Sie die heruntergeladene ZIP-Datei des Web-Plug-ins an.
7. Klicken Sie auf die Schaltfläche **Signatur hochladen**.

8. Geben Sie die heruntergeladene TXT-Datei für die Signatur des Web-Plug-ins an.

9. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Kaspersky Security Center überprüft die hochgeladenen Dateien und fügt das Web-Plug-in anschließend hinzu und installiert es.

10. Klicken Sie nach Abschluss der Installation auf **Uhrzeit der Verschlüsselung**.

Das Verwaltungs-Web-Plug-in wird mit der Standardkonfiguration installiert und in der Liste mit Verwaltungs-Web-Plug-ins angezeigt.

Installationspakete aus einer Datei erstellen

Mit benutzerdefinierten Installationspaketen können Sie die folgenden Aufgaben ausführen:

- Um ein beliebiges Programm (wie einen Text-Editor) auf einem Client-Gerät zu installieren, beispielsweise mithilfe einer Aufgabe.
- Zum Erstellen eines autonomen Installationspakets.

Ein benutzerdefiniertes Installationspaket ist ein Ordner mit einem Satz von Dateien. Die Quelle, aus der ein benutzerdefiniertes Installationspaket erstellt wird, ist eine *Archivdatei*. Die Archivdatei enthält eine Datei oder mehrere Dateien, die in das benutzerdefinierte Installationspaket aufgenommen werden müssen.

Wenn Sie ein benutzerdefiniertes Installationspaket erstellen, können Sie Befehlszeilenparameter angeben, z. B. um das Programm im Silent-Modus zu installieren.

So erstellen Sie ein benutzerdefiniertes Installationspaket:

1. Führen Sie eine der folgenden Aktionen aus:

   - Wechseln Sie zu **GERÄTESUCHE UND SOFTWAREVERTEILUNG → SOFTWAREVERTEILUNG UND ZUWEISUNG → INSTALLATIONSPAKETE**.
   - Wechseln Sie 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 Archivnamen an und klicken Sie auf **Durchsuchen**.

5. Wählen Sie im angezeigten Fenster eine Archivdatei aus, die sich auf den verfügbaren Datenträgern befindet.

   Sie können eine Archivdatei zip-, cab-, tar- oder tar.gz-Format hochladen. Es ist nicht möglich, ein Installationspaket aus einer sfx-Datei (selbstextrahierendes Archiv) zu erstellen.

   Das Hochladen der Datei auf den Administrationsserver wird gestartet.

6. Wenn Sie die Datei einer Kaspersky-App angegeben haben, werden Sie möglicherweise aufgefordert, den Endbenutzer-Lizenzvertrag (EULA) für die App zu lesen und zu akzeptieren. Um fortzufahren, müssen Sie den Endbenutzer-Lizenzvertrag akzeptieren. Wählen Sie die Option **Die Bedingungen und Bestimmungen des Endbenutzer-Lizenzvertrags akzeptieren** aus, wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags vollständig gelesen haben, und sie verstehen und akzeptieren.

   Darüber hinaus werden Sie möglicherweise aufgefordert, die Datenschutzrichtlinie zu lesen und zu akzeptieren. Um fortzufahren, müssen Sie die Datenschutzrichtlinie akzeptieren. Wählen Sie die Option **Ich akzeptiere die Datenschutzrichtlinie** nur dann aus, wenn Ihnen bewusst ist und Sie damit einverstanden sind, dass Ihre Daten so verarbeitet und (einschließlich in Drittländer) übertragen werden, wie es in der Datenschutzrichtlinie beschrieben ist.

7. Wählen Sie auf der nächsten Seite des Assistenten eine Datei aus (aus der Liste der Dateien, die aus der ausgewählten Archivdatei extrahiert wurden) und geben Sie die Befehlszeilenparameter einer ausführbaren Datei an.

   Sie können bestimmte Befehlszeilenparameter angeben, um das Programm im Silent-Modus aus dem Installationspaket zu installieren. Die Angabe von Befehlszeilenparametern ist optional.

   Das Erstellen des Installationspakets wird gestartet.

   Der Assistent meldet, wenn der Vorgang abgeschlossen ist.

   Falls das Installationspaket nicht erstellt wurde, wird eine entsprechende Meldung angezeigt.

8. Klicken Sie auf die Schaltfläche **Fertigstellen**, um den Assistenten zu schließen.

Das von Ihnen erstellte Installationspaket wird in den Unterordner "Pakete" des Freigegebenen Ordners des Administrationsservers heruntergeladen. Nach dem Herunterladen erscheint das Installationspaket in der Liste der Installationspakete.

Wenn Sie in der Liste der Installationspakete, die auf dem Administrationsserver verfügbar sind, auf den Link mit dem Namen eines benutzerdefinierten Installationspakets klicken, können Sie:

- Anzeigen der folgenden Eigenschaften eines Installationspakets:
  - **Das APNs-Zertifikat läuft bald ab**. 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 Installationspakets.
  - **Betriebssystem**. Typ des Betriebssystems, für welches das Installationspaket vorgesehen ist.
  - **Erstellt**. Erstellungsdatum des Installationspaketes.
  - **Geändert**. Änderungsdatum des Installationspaketes.
  - **Typ**. Typ des Installationspakets.
- Ändern Sie die Befehlszeilenparameter.

Autonome Installationspakete erstellen

Sie und die Gerätebenutzer in Ihrem Unternehmen können autonome Installationspakete verwenden, um Anwendungen manuell auf Geräten zu installieren.

Ein autonomes Installationspaket ist eine ausführbare Datei (Installer.exe). Sie können diese Datei auf dem Webserver oder im freigegebenen Ordner speichern, per E-Mail verschicken oder auf andere Weise an ein Client-Gerät übertragen. Auf dem Client-Gerät kann der Benutzer die empfangene Datei lokal ausführen, um ohne Beteiligung von Kaspersky Security Center Linux ein Programm zu installieren. Sie können autonome Installationspakete für Programme von Kaspersky und für Drittanbieter-Programme erstellen. Um ein autonomes Installationspaket für ein Drittanbieter-Programm zu erstellen, müssen Sie ein benutzerdefiniertes Installationspaket erstellen.

Stellen Sie sicher, dass unbefugte Personen keinen Zugriff auf das autonome Installationspaket haben.

So erstellen Sie ein autonomes Installationspaket:

1. Führen Sie eine der folgenden Aktionen aus:

   - Wechseln Sie zu **GERÄTESUCHE UND SOFTWAREVERTEILUNG → SOFTWAREVERTEILUNG UND ZUWEISUNG → INSTALLATIONSPAKETE**.
   - Wechseln Sie zu **VORGÄNGE → DATENVERWALTUNG → INSTALLATIONSPAKETE**.

   Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

2. Wählen Sie in der Liste der Installationspakete ein Installationspaket aus und klicken Sie oberhalb der Liste auf **Verteilen**.

3. Wählen Sie die Option **Unter Nutzung eines autonomen Pakets** aus.

   Daraufhin wird der Assistent für das Erstellen eines autonomen Installationspakets gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

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

5. Auf der Seite **In die Liste mit verwalteten Geräten verschieben** des Assistenten ist standardmäßig 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.

6. Nachdem die Erstellung des autonomen Installationspakets abgeschlossen wurde, klicken Sie auf der nächsten Seite des Assistenten auf **FERTIGSTELLEN**.

   Der Assistent für das Erstellen eines autonomen Installationspakets wird geschlossen.

Das autonome Installationspaket wird im Unterordner PkgInst des Freigegebenen Ordners des Administrationsservers erstellt und abgelegt. Sie können eine Liste der autonomen Pakete anzeigen. Klicken Sie dazu oberhalb der Liste der Installationspakete auf **Liste der autonomen Pakete anzeigen**.

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:

Klicken Sie oberhalb der Liste auf die Schaltfläche **Liste der autonomen Pakete anzeigen**.

In der Liste der autonomen Installationspakete werden die folgenden Eigenschaften angezeigt:

- **Archivname**. Name des autonomen Installationspaketes, der automatisch aus dem Namen der im Paket enthaltenen Anwendung und der Anwendungsversion gebildet wird.

- **Programmname**. Programmname, der in dem autonomen Installationspaket enthalten ist.

- **Programmversion**.

- **Name des Installationspakets des Administrationsagenten**. Diese Eigenschaft wird nur angezeigt, wenn in dem autonomen Installationspaket der Administrationsagent enthalten ist.

- **Version des Administrationsagenten**. Diese Eigenschaft wird nur angezeigt, wenn in dem autonomen Installationspaket der Administrationsagent enthalten ist.

- **Größe**. Dateigröße (MB).

- **Gruppe**. Name der Gruppe, in die das Client-Gerät nach der Installation des Administrationsagenten verschoben wird.

- **Erstellt**. Datum und Uhrzeit der Erstellung des autonomen Installationspakets.
- **Geändert**. Datum und Uhrzeit der Änderung des autonomen Installationspakets.
- **Pfad**. Vollständiger Pfad des Ordners, in dem sich das autonome Installationspaket befindet.
- **Webadresse**. Webadresse des Speicherorts für das autonome Installationspaket.
- **Dateihash**. Mit dieser Eigenschaft wird bestätigt, dass das eigenständige Installationspaket nicht von Dritten geändert wurde und der Benutzer dieselbe Datei erhalten hat, die Sie erstellt und an den Benutzer übertragen haben.

So zeigen Sie die Liste der autonomen Installationspakete für ein bestimmtes Installationspaket an:

Wählen Sie in der Liste das Installationspaket aus und klicken Sie auf die Schaltfläche **Liste der autonomen Pakete anzeigen** über der Liste.

In der Liste der autonomen Installationspakete können Sie:

- Veröffentlichung eines autonomen Installationspakets auf dem "Web Server" durch Klick auf **Veröffentlichen**. Ein veröffentlichtes autonomes Installationspaket kann von jenen Benutzern heruntergeladen werden, denen Sie einen Link für dieses autonome Installationspaket geschickt haben.
- Aufheben der Veröffentlichung eines autonomen Installationspakets auf dem "Web Server" durch Klick auf **Veröffentlichung aufheben**. Ein unveröffentlichtes autonomes Installationspaket kann nur von Ihnen selbst und von anderen Administratoren heruntergeladen werden.
- Laden Sie ein autonomes Installationspaket auf Ihr Gerät herunter, indem Sie auf die Schaltfläche **Herunterladen** klicken.
- Senden einer E-Mail-Nachricht mit einem Link für das autonome Installationspaket durch Klick auf **Per E-Mail senden**.
- Löschen Sie ein autonomes Installationspaket, indem Sie auf die Schaltfläche **Entfernen** klicken.

Programme mit der Aufgabe zur Remote-Installation installieren

Mit Kaspersky Security Center Linux können Sie Programme auf anderen Geräten per Fernzugriff installieren. Dazu dienen Aufgaben zur Remote-Installation. Mithilfe des Assistenten werden die Aufgaben erstellt und den Geräten zugewiesen. Um den Geräten schneller und einfacher eine Aufgabe zuzuweisen, können Sie die Geräte im Fenster des Assistenten auf die von Ihnen bevorzugte Art festlegen:

- **Geräte auswählen, die vom Administrationsserver erkannt wurden**. In diesem Fall wird die Aufgabe einer Reihe von Geräten zugewiesen. In dieser Reihe von Geräten können Sie sowohl Geräte aus den Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- **Geräteadressen manuell angeben oder aus Liste importieren**. Sie können DNS-Namen, IP-Adressen und IP-Subnetze der Geräte angeben, denen die Aufgabe zugewiesen werden soll.
- **Aufgabe einer Geräteauswahl zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Auswahl gehören. Sie können eine standardmäßig erstellte Auswahl oder Ihre eigene Auswahl angeben.

- **Aufgabe einer Administrationsgruppe zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Administrationsgruppe gehören.

Für eine korrekte Ausführung der Aufgabe der Remote-Installation auf einem Gerät, auf dem der Administrationsagent nicht installiert ist, müssen die folgenden Ports geöffnet werden: TCP 139 und 445 sowie UDP 137 und 138. Diese Ports sind standardmäßig auf allen Geräten geöffnet, die zur Domäne gehören. Sie werden automatisch mithilfe des Tools zur Vorbereitung der Geräte auf die Remote-Installation geöffnet.

Ein Programm auf bestimmten Geräten installieren

Dieser Abschnitt enthält Informationen darüber, wie ein Programm in einer Administrationsgruppe, Geräte mit bestimmten IP-Adressen oder eine Auswahl verwalteter Geräte per Fernzugriff installiert werden.

Um ein Programm auf ausgewählten Geräten zu installieren:

1. Stellen Sie eine Verbindung zum Administrationsserver her, der die gewünschten Geräte verwaltet.
2. Wechseln Sie im Hauptmenü zu **GERÄTE** → **AUFGABEN**.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent zum Hinzufügen von Aufgaben wird gestartet.
4. Wählen Sie im Feld **Aufgabentyp** die Variante **Remote-Installation eines Programms** aus.
5. Wählen Sie eine der folgenden Varianten 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 DNS-Namen, IP-Adressen und IP-Subnetze der Geräte angeben, denen die 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. Folgen Sie den Anweisungen des Assistenten.

   Der Assistent für das Hinzufügen einer Aufgabe erstellt eine Aufgabe, mit der das im Assistenten ausgewählte Programm per Fernzugriff auf den angegebenen Geräten installiert werden kann. Wenn Sie Option **Aufgabe einer Administrationsgruppe zuweisen** ausgewählt haben, ist die Aufgabe eine Gruppenaufgabe.

7. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen festgelegten Zeitplan gestartet wird.

Nach Abschluss der Remote-Installationsaufgabe wurde das ausgewählte Programm auf den angegebenen Geräten installiert.

Programme mit Gruppenrichtlinien des Active Directory installieren

Mit Kaspersky Security Center können Sie Programme von Kaspersky auf verwalteten Geräten mithilfe der Gruppenrichtlinien des Active Directory installieren.

Sie können Programme mithilfe der Gruppenrichtlinien des Active Directory nur aus Installationspaketen installieren, die den Administrationsagenten enthalten.

Um ein Programm mithilfe von Active Directory-Gruppenrichtlinien zu installieren:

1. Starten Sie den Assistenten für die Bereitstellung des Schutzes. Folgen Sie den Anweisungen des Assistenten.

2. Aktivieren Sie auf der Seite **Einstellungen für die Aufgabe zur Remote-Installation** des Assistenten für die Bereitstellung des Schutzes die Option **Installation des Installationspakets in Active Directory-Gruppenrichtlinien festlegen**.

3. Aktivieren Sie auf der Seite **Benutzerkonten für den Zugriff auf Geräte auswählen** die Option **Benutzerkonto erforderlich (Administrationsagent wird nicht verwendet)**.

4. Fügen Sie das entweder Benutzerkonto mit Administratorberechtigungen auf dem Gerät, auf dem Kaspersky Security Center installiert ist hinzu, oder das Benutzerkonto, das in der Domänengruppe der Group Policy Creators Owners beinhaltet ist.

5. Gewähren Sie dem ausgewählten Benutzerkonto die Berechtigungen:

   a. Gehen Sie zu **Systemsteuerung** → **Verwaltung** → **Verwaltung von Gruppenrichtlinien**.

   b. Klicken Sie auf den Knoten mit dem gewünschten Namen.

   c. Klicken Sie auf den Abschnitt **Delegieren**.

   d. Wählen Sie in der Dropdown-Liste **Berechtigung** die Option **GPOs verlinken** aus.

   e. Klicken Sie auf **Hinzufügen**.

   f. Wählen Sie im neuen Fenster **Benutzer, Computer oder Gruppe auswählen** das gewünschte Benutzerkonto.

   g. Klicken Sie auf **OK**, um das Fenster **Benutzer, Computer oder Gruppe auswählen** zu schließen.

h. Wählen Sie in der Liste **Benutzer und Gruppen** das Konto, dass Sie gerade hinzugefügt haben und klicken Sie anschließend auf **Erweitert** → **Erweitert**.

i. Doppelklicken Sie in der Liste **Berechtigungseinträge** auf das Konto, dass Sie gerade hinzugefügt haben.

j. Gewähren Sie die folgenden Berechtigungen:

- **Erstellen von Gruppenobjekten**
- **Löschen von Gruppenobjekten**
- **Objekte für Gruppenrichtliniencontainer erstellen**
- **Objekte für Gruppenrichtliniencontainer löschen**

k. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

6. Legen Sie die weiteren Einstellungen fest, indem Sie den Anweisungen des Assistenten folgen.
7. Starten Sie die erstellte Aufgabe zur Remote-Installation manuell oder gemäß einem Zeitplan.

Daraufhin wird die Remote-Installation auf folgende Weise ausgeführt:

1. Nach dem Start der Aufgabe werden in jeder Domäne, zu der Client-Geräte für diese Aufgabe zur Remote-Installation gehören, folgende Objekte angelegt:
   - Group policy object (GPO) mit dem Namen **Kaspersky_AK{GUID}**.
   - Eine Sicherheitsgruppe, die dem GPO entspricht. Diese Sicherheitsgruppe umfasst Client-Geräte, auf die sich die Aufgabe erstreckt. Die Zusammensetzung der Sicherheitsgruppe bestimmt den Geltungsbereich des GPOs.
2. Kaspersky Security Center installiert die Kaspersky-Programme auf den Client-Geräten direkt aus dem freigegeben Netzwerkordner "Share" des Programms. Im Installationsordner von Kaspersky Security Center wird dabei ein untergeordneter Hilfsordner erstellt, der die msi-Datei für das zu installierende Programm enthält.
3. Beim Hinzufügen neuer Geräte zum Gültigkeitsbereich der Aufgabe werden diese erst beim nächsten Start der Aufgabe zur entsprechenden Sicherheitsgruppe hinzugefügt. Wenn die Option **Übersprungene Aufgaben starten** aktiviert ist, werden die Geräte sofort zur Sicherheitsgruppe hinzugefügt.
4. Beim Löschen von Geräten aus dem Gültigkeitsbereich einer Aufgabe werden sie erst beim nächsten Start der Aufgabe aus der Sicherheitsgruppe gelöscht.
5. Beim Löschen einer Aufgabe aus dem Active Directory werden auch das GPO, der Link für das GPO und die entsprechende Sicherheitsgruppe gelöscht.

Wenn Sie ein anderes Installationsschema über Active Directory verwenden möchten, können Sie die Einstellungen manuell ändern. Das kann in folgenden Fällen nötig werden:

- Wenn der Administrator für den Antiviren-Schutz nicht die nötigen Rechte besitzt, um im Active Directory einiger Domänen Änderungen vorzunehmen.
- Wenn das ursprüngliche Installationspaket auf einer separaten Netzwerkressource gespeichert werden soll.
- Wenn ein GPO konkreten Unterabteilungen des Active Directory zugewiesen werden soll.

Folgende alternative Installationsschemata über Active Directory sind verfügbar:

- Falls die Installation direkt aus dem freigegebenen Ordner von Kaspersky Security Center erfolgen soll, muss in den Eigenschaften des GPO eine msi-Datei angegeben werden, die sich im exec-Unterordner des Ordners des Installationspakets für das erforderliche Programm befindet.

- Wenn das Installationspaket in einer anderen Netzwerkressource gespeichert werden muss, kopieren Sie den ganzen Inhalt des Ordners exec in das Paket, weil der Ordner neben der msi-Datei die Konfigurationsdateien enthält, die beim Anlegen des Installationspakets erstellt wurden. Um den Lizenzschlüssel zusammen mit dem Programm zu installieren, kopieren Sie auch die Schlüsseldatei in den Ordner.

Programme auf sekundären Administrationsservern installieren

Um ein Programm auf sekundären Administrationsservern zu installieren:

1. Stellen Sie eine Verbindung zum Administrationsserver her, der die gewünschten sekundären Administrationsserver verwaltet.

2. Vergewissern Sie sich, dass sich das zum Programm passende Installationspaket auf jedem der gewählten sekundären Administrationsserver befindet. Wenn Sie das Installationspaket auf keinem der sekundären Server finden können, verteilen Sie es. Erstellen Sie dazu eine Aufgabe mit dem Aufgabentyp **Installationspaket verteilen**.

3. Erstellen Sie eine Aufgabe zur Remote-Installation des Programms auf den sekundären Administrationsservern. Wählen Sie den Installationstyp **Remote-Installation eines Programms auf sekundärem Administrationsserver** aus.

   Der Assistent für das Hinzufügen einer Aufgabe erstellt eine Aufgabe, mit der das im Assistenten ausgewählte Programm per Fernzugriff auf den angegebenen sekundären Administrationsservern installiert werden kann.

4. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen festgelegten Zeitplan gestartet wird.

Nach Abschluss der Remote-Installationsaufgabe wurde das ausgewählte Programm auf den angegebenen sekundären Administrationsservern installiert.

Einstellungen für die Remote-Installation auf Unix-Geräten angeben

Wenn Sie ein Programm mithilfe einer Remote-Installationsaufgabe 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 Remote-Installationsaufgabe an:

1. Wechseln Sie im Hauptmenü zu **GERÄTE** → **AUFGABEN**.

2. Klicken Sie auf den Namen der Remote-Installationsaufgabe, 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. Legen Sie die folgenden Einstellungen fest:

   - **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 14 Linux 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 14 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 14 Linux 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 Schutzprogrammen von Drittanbietern

Zur Installation der Sicherheitsanwendungen von Kaspersky mithilfe von Kaspersky Security Center Linux ist es möglicherweise erforderlich, Drittanbietersoftware zu löschen, die mit dem zu installierenden Programm nicht kompatibel ist. Kaspersky Security Center 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 im Assistenten für die Bereitstellung des Schutzes konfigurieren. Wenn diese Option aktiviert ist, entfernt Kaspersky Security Center vor der Installation einer Sicherheitsanwendung auf dem verwalteten Gerät inkompatible Programme.

Anleitungen: Inkompatible Programme vor der Installation entfernen

Löschen der inkompatiblen Programme mithilfe einer separaten Aufgabe

Zum Löschen der inkompatiblen Programme wird die Aufgabe **Remote-Deinstallation des Programms** verwendet. Die Aufgabe muss vor der Aufgabe zur Installation des Schutzprogramms 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.

Anleitungen: Eine Aufgabe erstellen

Remote-Entfernen von Programmen und Software-Updates

Sie können Programme oder Software-Updates auf verwalteten Geräten, auf denen Linux ausgeführt wird, nur per Fernzugriff über den Administrationsagenten entfernen.

Um Programme oder Software-Updates von ausgewählten Geräten remote zu entfernen:

1. Wählen Sie im Hauptfenster des Programms **GERÄTE** → **AUFGABEN**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent zum Hinzufügen von Aufgaben wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.
3. Wählen Sie für Kaspersky Security Center den Aufgabentyp **Remote-Deinstallation eines Programms**.
4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen.

   Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.
5. Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll.
6. Wählen Sie aus, welche Art von Software Sie entfernen wollen, und wählen Sie anschließend bestimmte Programme, Updates oder Patches aus, die Sie entfernen wollen:

   - **Verwaltetes Programm deinstallieren**

     Eine Liste mit Kaspersky-Programmen angezeigt. Wählen Sie das Programm aus, das Sie entfernen möchten.

   - **Inkompatibles Anwendung deinstallieren**

     Eine Liste mit Programmen, die nicht kompatibel zu Kaspersky-Sicherheitsanwendungen oder zu Kaspersky Security Center sind, wird angezeigt. Aktivieren Sie die Kontrollkästchen neben den Programmen, die Sie entfernen möchten.

   - **Programm aus der Programm-Registry deinstallieren**

Standardmäßig übertragen Administrationsagenten die Information über Programme, die auf verwalteten Geräten installiert sind, an den Administrationsserver. Die Liste der installierten Programme ist in der Programm-Registry. gespeichert.

Um ein Programm von der Programm-Registry auszuwählen:

a. Klicken Sie auf das Feld **Zu deinstallierendes Programm** und wählen Sie anschließend das Programm aus, welches Sie entfernen wollen.

b. Geben Sie die folgenden Optionen für die Deinstallation an:

- Deinstallationsmodus

  Wählen Sie aus, wie Sie das Programm entfernen möchten:

  - **Deinstallationsbefehl automatisch definieren**

    Wenn das Programm einen Deinstallationsbefehl besitzt, welcher durch den Hersteller des Programms vorgegeben wurde, nutzt Kaspersky Security Center diesen Befehl. Es wird empfohlen, diese Option auszuwählen.

  - **Deinstallationsbefehl angeben**

    Wählen Sie diese Option aus, wenn Sie Ihren eigenen Befehl für die Deinstallation des Programms angeben möchten.

    Es wird empfohlen, das Entfernen des Programms zunächst unter Verwendung der Option **Deinstallationsbefehl automatisch definieren** auszuprobieren. Sollte die Deinstallation mittels automatisch definierten Befehl fehlschlagen, verwenden Sie Ihren eigenen Befehl.

    Geben Sie einen Installationsbefehl in das Feld ein und geben Sie anschließend folgende Optionen an:

    Diesen Deinstallationsbefehl nur dann verwenden, wenn der Standardbefehl nicht automatisch entdeckt wurde

    Kaspersky Security Center prüft, ob das ausgewählte Programm einen vom Programmhersteller vorgegeben Deinstallationsbefehl besitzt. Wenn so ein Befehl existiert, verwendet Kaspersky Security Center diesen anstelle des Befehls der in dem Feld **Deinstallationsbefehl des Programms** angegeben wurde.

    Es wird empfohlen, diese Option zu aktivieren.

- Nach einer erfolgreichen Deinstallation einen Neustart durchführen

  Wenn der Vorgang nach einer erfolgreichen Deinstallation einen Neustart des Betriebssystems auf dem verwalteten Gerät benötigt, wird das Betriebssystem automatisch neu gestartet.

7. Geben Sie an, auf welche Weise Client-Geräte das Tool für die Deinstallation herunterladen sollen:

- Unter Nutzung des Administrationsagenten

Die Dateien werden den Client-Geräten mithilfe des Administrationsagenten, der auf den Geräten installiert ist, ausgeliefert.

Wenn diese Option deaktiviert ist, werden die Dateien über Tools des Linux-Betriebssystems ausgeliefert.

Es wird empfohlen, die Option zu aktivieren, wenn die Aufgabe für Geräte mit installierten Administrationsagenten vorgesehen ist.

- Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver

  Die Option ist veraltet. Verwenden Sie stattdessen die Option **Unter Nutzung des Administrationsagenten** oder **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**.

  Die Dateien werden mit den Betriebssystem-Tools des Administrationsservers an die Client-Geräte übertragen. Diese Option kann aktiviert werden, wenn auf dem Client-Gerät kein Administrationsagent installiert ist, das Client-Gerät sich aber im selben Netzwerk wie der Administrationsserver befindet.

- Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte

  Die Dateien werden den Client-Geräten mithilfe der Tools von den Betriebssysteme durch Verteilungspunkte ausgeliefert. Diese Option kann aktiviert werden, wenn sich im Netzwerk mindestens ein Verteilungspunkt befindet.

  Ist die Option **Unter Nutzung des Administrationsagenten** aktiviert, werden die Dateien nur dann mit den Betriebssystem-Tools zugestellt, wenn die Funktionen des Administrationsagenten nicht verwendet werden können.

- Maximale Anzahl gleichzeitiger Downloads

  Die erlaubte Maximalanzahl an Client-Geräten, an die der Administrationsserver simultan Dateien ausliefern kann. Je höher die Nummer, umso schneller werden die Programme deinstalliert, aber umso höher ist auch die Auslastung des Administrationsservers.

- Maximale Anzahl der Deinstallationsversuche

Wenn während der Ausführung der Aufgabe *Remote-Deinstallation eines Programms* für Kaspersky Security Center die Anzahl an Deinstallationsversuchen einer Anwendung auf einem verwalteten Gerät nicht innerhalb der Anzahl an Versuchen, die im Parameter angegeben wurde, erfolgreich ist, stoppt Kaspersky Security Center das Ausliefern des Deinstallationstools auf diesem verwalteten Gerät und startet die Installationsaufgabe auf dem Gerät nicht mehr.

Der Parameter **Maximale Anzahl der Deinstallationsversuche** ermöglicht es Ihnen, die Ressourcen eines verwalteten Geräts zu sparen und den Datenverkehr zu reduzieren (Deinstallation, MSI-Datei ausführen und Fehlermeldungen).

Wiederholende Versuche zum Start der Aufgabe können auf ein Problem auf dem Gerät hinweisen, dass die Deinstallation verweigert. Der Administrator sollte das Problem innerhalb der angegeben Anzahl an Deinstallationsversuchen lösen und anschließend die Aufgabe neu starten (manuell oder mittels Zeitplan).

Wenn die Deinstallation nicht abgeschlossen werden kann, ist das Problem unter Umständen nicht lösbar und jeder weitere Aufgabenstart wird als kostspielig im Sinne unnützen Verbrauchs von Ressourcen und Datenverkehr betrachtet.

Beim Erstellen der Aufgabe wird der Zähler für die Versuche auf `0` gesetzt. Jede Ausführung des Installers, die einen Fehler zurückliefert erhöht den Zählerstand.

Wenn die im Parameter angegebene Anzahl an Versuchen überschritten wurde und das Gerät für die Deinstallation der Anwendung bereit ist, können Sie den Wert der **Maximale Anzahl der Deinstallationsversuche** erhöhen und die Aufgabe zu Deinstallation der Anwendung starten. Alternativ können Sie eine neue Aufgabe des Typs *Remote-Deinstallation eines Programms* erstellen.

- Typ des Betriebssystems vor dem Download prüfen

  Bevor die Dateien auf die Client-Geräte übertragen werden, prüft Kaspersky Security Center, ob die Einstellungen des Deinstallationstools auf dem Betriebssystem des Client-Geräts anwendbar sind. Wenn die Einstellungen nicht anwendbar sind, überträgt Kaspersky Security Center die Dateien nicht und wird nicht versuchen, die Anwendung zu deinstallieren. So können Sie beispielsweise ein Programm von Geräten einer Administrationsgruppe, die mehrere Geräte mit unterschiedlichen Betriebssystemen enthält, deinstallieren, indem Sie die Aufgabe zur Deinstallation der Administrationsgruppe zuweisen und anschließend die Option zum Überspringen von Geräten mit davon abweichenden Betriebssystemen aktivieren.

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.

- 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. Bei Bedarf können Sie Benutzerkonten hinzufügen, die für den Start der Aufgabe zur Remote-Deinstallation verwendet werden sollen:

   - **Kein Benutzerkonto erforderlich (Administrationsagent ist installiert)**

     Wenn diese Variante ausgewählt ist, muss das Benutzerkonto nicht angegeben werden, unter dem das Installationsprogramm 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)**

     Wenn diese Variante ausgewählt ist, kann das Konto angegeben werden, unter dem das Installationsprogramm gestartet werden soll. Das Benutzerkonto kann für den Fall angegeben werden, dass der Administrationsagent auf den Geräten, für die diese Aufgabe vorgesehen ist, nicht installiert ist.

     Sie können mehrere Benutzerkonten angeben, wenn beispielsweise kein Konto 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.

     Wenn kein Benutzerkonto hinzugefügt wurde, wird die Aufgabe unter dem Benutzerkonto gestartet, unter dem der Dienst des Administrationsservers ausgeführt 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 an.

14. Klicken Sie auf die Schaltfläche **Speichern**.

15. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen vorgegebenen Zeitplan gestartet wurde.

Nach Fertigstellung der Aufgabe zur Remote-Deinstallation wird das gewählte Programm von den ausgewählten Geräten entfernt.

Ein Gerät mit SUSE Linux Enterprise Server 15 für die Installation des Administrationsagenten vorbereiten

Um den Administrationsagenten auf einem Gerät mit dem Betriebssystem SUSE Linux Enterprise Server 15 zu installieren:

Führen Sie vor der Installation des Administrationsagenten den folgenden Befehl aus:

```
$ sudo zypper install insserv-compat
```

Dies erlaubt Ihnen die Installation des Pakets insserv-compat, um den Administrationsagenten richtig zu konfigurieren.

Führen Sie den Befehl `rpm -q insserv-compat` aus, um zu prüfen, ob das Paket bereits installiert ist.

Wenn Ihr Netzwerk viele Geräte mit SUSE Linux Enterprise Server 15 umfasst, können Sie das spezielle Programm zum Konfigurieren und Verwalten der Unternehmensinfrastruktur verwenden. Mittels dieses Programms können Sie das Paket insserv-compat automatisch auf allen erforderlichen Geräten gleichzeitig installieren. Sie können beispielsweise Puppet, Ansible, Chef oder Ihr selbsterstelltes Skript verwenden – je nachdem, was für Sie am besten geeignet ist.

Nachdem Sie das SUSE Linux Enterprise Server 15-Gerät vorbereitet haben, stellen Sie den Administrationsagenten bereit und installieren ihn.

Programme von Kaspersky: Lizenzierung und Aktivierung

Dieser Abschnitt beschreibt die Funktionen von Kaspersky Security Center, die sich auf die Arbeit mit den Lizenzschlüsseln von verwalteten Kaspersky-Programmen beziehen.

Kaspersky Security Center Linux ermöglicht eine zentrale Verteilung von Lizenzschlüsseln für Kaspersky-Programme auf Client-Geräte sowie die Überwachung der Schlüsselverwendung und die Verlängerung von Lizenzen.

Beim Hinzufügen eines Lizenzschlüssels über Kaspersky Security Center 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.

Lizenzierung der verwalteten Programme

Jedes der auf den verwalteten Geräten installierten Kaspersky-Programme muss mit einer Schlüsseldatei oder einem Aktivierungscode lizenziert werden. Eine Schlüsseldatei oder ein Aktivierungscode kann folgendermaßen bereitgestellt werden:

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

Sie können mit einer der oben aufgeführten Methoden einen neuen aktiven Lizenzschlüssel oder einen Reserve-Lizenzschlüssel hinzufügen. Kaspersky-Programme verwenden zum aktuellen Zeitpunkt einen aktiven Schlüssel und speichern einen Reserve-Schlüssel, der nach Ablauf des aktiven Schlüssels angewendet wird. 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.

Mittels automatischer Verteilung

Wenn Sie verschiedene verwaltete Programme verwenden und eine bestimmte Schlüsseldatei oder Aktivierungscode an die Geräte verteilen möchten, verwenden Sie andere Methoden zur Verteilung des Aktivierungscodes oder der Schlüsseldatei.

Kaspersky Security Center erlaubt die automatische Verteilung der vorhandenen Lizenzschlüssel an die Geräte. Angenommen, in der Datenverwaltung des Administrationsservers befinden sich drei Lizenzschlüssel. Sie haben die Option **Automatisch zu verteilender Lizenzschlüssel** für alle drei Lizenzschlüssel aktiviert. Auf den Unternehmensgeräten ist eine Sicherheitsanwendung von Kaspersky installiert, z. B. Kaspersky Endpoint Security für Linux. Ein neues Gerät wurde entdeckt und erfordert die Bereitstellung eines Lizenzschlüssels. Das Programm ermittelt, dass für dieses Gerät z. B. zwei Lizenzschlüssel aus dem Speicher geeignet sind: Lizenzschlüssel *Key_1* und Lizenzschlüssel *Key_2*. Einer dieser Lizenzschlüssel wird an das Gerät verteilt. In diesem Fall kann nicht vorausgesagt werden, welcher der beiden Lizenzschlüssel an das Gerät verteilt werden wird, da die automatische Verteilung von Lizenzschlüsseln keinerlei Aktivitäten des Administrators vorsieht.

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

Vor der Verteilung muss die Schlüsseldatei oder Aktivierungscode zur Datenverwaltung des Administrationsservers hinzugefügt werden.

Anleitung:

- Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen
- Lizenzschlüssel automatisch verteilen

Hinzufügen einer Schlüsseldatei oder eines Aktivierungscodes zum Installationspaket eines verwalteten Programms

Diese Option wird aus Sicherheitsgründen nicht empfohlen. Eine Schlüsseldatei oder ein Aktivierungscode, der zum Installationspaket hinzugefügt wurde, kann kompromittiert werden.

Wenn die Installation des verwalteten Programms mithilfe eines Installationspakets erfolgt, können Sie eine Schlüsseldatei oder einen Aktivierungscode im Installationspaket oder in der Richtlinie dieses Programms angeben. Der Lizenzschlüssel wird bei der nächsten Synchronisierung des Geräts mit dem Administrationsserver an die verwalteten Geräte verteilt.

Anleitungen: Lizenzschlüssel zu einem Installationspaket hinzufügen

Verteilung mithilfe der Aufgabe zum Hinzufügen eines Lizenzschlüssels für ein verwaltetes Programm

Wenn Sie die Aufgabe "Lizenzschlüssel hinzufügen" für verwaltete Programme verwenden, können Sie den Lizenzschlüssel auswählen, der an die Geräte verteilt werden soll, und die Geräte auf die von Ihnen bevorzugte Art auswählen, z. B. indem Sie eine Administrationsgruppe oder eine Geräteauswahl wählen.

Vor der Verteilung muss die Schlüsseldatei oder Aktivierungscode zur Datenverwaltung des Administrationsservers hinzugefügt werden.

Anleitung:

- 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.

Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen

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

1. Wechseln Sie im Hauptmenü zu **VORGÄNGE → LIZENZVERWALTUNG → LIZENZEN FÜR KASPERSKY-SOFTWARE**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Wählen Sie, was Sie hinzufügen möchten:
   - **Schlüsseldatei hinzufügen**

     Klicken Sie auf **Schlüsseldatei auswählen** und finden Sie die .key-Datei, die Sie hinzufügen möchten.
   - **Aktivierungscode eingeben**

     Geben Sie im Textfeld den Aktivierungscode an und klicken Sie auf **Senden**.
4. Klicken Sie auf die Schaltfläche **Schließen**.

Der oder die Lizenzschlüssel werden zur Datenverwaltung des Administrationsservers hinzugefügt.

Lizenzschlüssel auf Client-Geräte verteilen

Die Kaspersky Security Center 14 Web Console ermöglicht die Verteilung von Lizenzschlüsseln auf Client-Geräte mit der Aufgabe *Lizenzschlüssel verteilen*.

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 zum Hinzufügen von Aufgaben 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 Linux 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 → LIZENZVERWALTUNG → LIZENZEN FÜR KASPERSKY-SOFTWARE**.
2. Klicken Sie auf den Namen des Lizenzschlüssels, den Sie automatisch auf die Geräte verteilen möchten.
3. Aktivieren Sie im folgenden Eigenschaftenfenster des Lizenzschlüssels **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.
4. Klicken Sie auf die Schaltfläche **Speichern**.

   Der Lizenzschlüssel wird automatisch an alle kompatiblen Geräte verteilt.

Die Verteilung des Lizenzschlüssels erfolgt durch den Administrationsagenten. Für das Programm werden keine Aufgaben zur Verteilung eines Lizenzschlüssels erstellt.

Wenn ein Lizenzschlüssel 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 in dem Eigenschaftenfenster des Lizenzschlüssels das Kontrollkästchen **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** auswählen, wird sofort ein Lizenzschlüssel in Ihrem Netzwerk verteilt. Wenn Sie diese Option nicht auswählen, können Sie später manuell einen Lizenzschlüssel verteilen.

Informationen zu verwendeten Lizenzschlüsseln anzeigen

Um die Liste mit Lizenzschlüsseln anzuzeigen, die zur Datenverwaltung des Administrationsservers hinzugefügt wurden, gehen Sie wie folgt vor:

Wechseln Sie im Hauptmenü zu **VORGÄNGE → LIZENZVERWALTUNG → LIZENZEN FÜR KASPERSKY-SOFTWARE**.

Die angezeigte Liste enthält die Schlüsseldatei und Aktivierungscodes, die zur Datenverwaltung des Administrationsservers hinzugefügt wurden.

Um detaillierte Informationen über einen Lizenzschlüssel anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **VORGÄNGE → LIZENZVERWALTUNG → LIZENZEN FÜR KASPERSKY-SOFTWARE**.
2. Klicken Sie auf den Namen des gewünschten Lizenzschlüssels.

Im Eigenschaftenfenster des Lizenzschlüssels können Sie Folgendes ansehen:

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

Um zu sehen, welche Lizenzschlüssel auf einem bestimmten Client-Gerät bereitgestellt werden, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **GERÄTE → VERWALTETE GERÄTE**.
2. Klicken Sie auf den Namen des gewünschten Geräts.
3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts die Registerkarte **Programme** aus.
4. Klicken Sie auf den Namen des Programms, für das Sie Informationen über den Lizenzschlüssel anzeigen möchten.
5. Wählen Sie im folgenden Fenster mit den Programmeigenschaften die Registerkarte **Allgemein** und öffnen Sie dann den Abschnitt **Lizenz**.

Die wichtigsten Informationen über den aktiven Lizenzschlüssel und die Reserveschlüssel werden angezeigt.

Zur Bestimmung der aktuellen Einstellungen für die Lizenzschlüssel des virtuellen Administrationsservers sendet der Administrationsserver mindestens einmal pro Stunde eine Anfrage an die Aktivierungsserver von Kaspersky.

Lizenzschlüssel aus der Datenverwaltung löschen

Wenn Sie den aktiven Lizenzschlüssel löschen, der auf einem verwalteten Gerät bereitgestellt wird, bleibt die Anwendung auf dem verwalteten Gerät weiterhin funktionsfähig.

Um eine Schlüsseldatei oder einen Aktivierungscode aus der Datenverwaltung des Administrationsservers zu löschen, gehen Sie wie folgt vor:

1. Gehen Sie zu **VORGÄNGE → LIZENZVERWALTUNG → LIZENZEN FÜR KASPERSKY-SOFTWARE**.
2. Wählen Sie die Lizenzdatei oder den Aktivierungscode aus, den Sie aus der Datenverwaltung löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Bestätigen Sie den Vorgang mit der Schaltfläche **Uhrzeit der Verschlüsselung**.

Die ausgewählte Schlüsseldatei oder der Aktivierungscode wird aus der Datenverwaltung gelöscht.

Ein gelöschter Lizenzschlüssel kann erneut hinzugefügt werden, oder es kann ein anderer Lizenzschlüssel hinzugefügt werden.

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 deinstallieren.

So widerrufen Sie eine EULA für verwaltete Kaspersky-Programme:

1. Öffnen Sie das Eigenschaftenfenster des Administrationsservers und wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Endbenutzer-Lizenzverträge**.

   Es wird eine Liste der EULAs angezeigt, die beim Erstellen von Installationspaketen, bei der nahtlosen Installation von Updates oder bei der Bereitstellung von Kaspersky Security für mobile Endgeräte akzeptiert wurden.

2. Wählen Sie in der Liste die EULA aus, die Sie widerrufen möchten.

   Sie können die folgenden Eigenschaften der EULA anzeigen:

   - Datum, an dem die EULA akzeptiert wurde.
   - Name des Benutzers, der die EULA akzeptiert hat.

3. Klicken Sie auf das Datum, an dem die EULA akzeptiert wurde, um ihr Eigenschaftenfenster mit den folgenden Informationen anzuzeigen:

   - Name des Benutzers, der die EULA akzeptiert hat.
   - Datum, an dem die EULA akzeptiert wurde.
   - Eindeutige ID (UID) der EULA.
   - Vollständiger Text der EULA.
   - Liste der mit der EULA verbundenen Objekte (Installationspakete, nahtlose Updates, Mobile Apps) und ihrer entsprechenden Namen und Typen.

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

   > Sollten Objekte (Installationspakete und ihre entsprechenden Aufgaben) existieren, die den Widerruf der EULA verhindern, wird eine entsprechende Nachricht angezeigt. Sie können den Widerruf erst fortsetzen, wenn Sie diese Objekte gelöscht haben.

   In dem sich öffnenden Fenster werden Sie darüber informiert, dass Sie zunächst das Kaspersky-Programm deinstallieren müssen, welches dieser EULA entspricht.

5. Klicken Sie auf die Schaltfläche, um den Widerruf zu bestätigen.

Die EULA wurde widerrufen. Sie wird nicht länger in der Liste der 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.

So verlängern Sie Lizenzen, die entweder abgelaufen oder kurz vor dem Ablaufen sind:

1. Führen Sie eine beliebige der folgenden Aktionen aus:

   - Wechseln Sie im Hauptmenü zu **VORGÄNGE → LIZENZVERWALTUNG → LIZENZEN FÜR KASPERSKY-SOFTWARE**.

   - Wechseln Sie im Hauptmenü zu **ÜBERWACHUNG UND BERICHTERSTATTUNG → DASHBOARD** und klicken Sie anschließend auf den Link **Ablaufende Lizenzen anzeigen** neben einer Benachrichtigung.

   Es öffnet sich das Fenster **LIZENZEN FÜR KASPERSKY-SOFTWARE**, in dem Sie Lizenzen anzeigen und erneuern können.

2. Klicken Sie neben der erforderlichen Lizenz auf den Link **Lizenz verlängern**.

   Durch Klicken des Links zur Verlängerung der Lizenz erklären Sie sich damit einverstanden, die folgenden Informationen über das Kaspersky Security Center an Kaspersky zu übertragen: die Version, die verwendete Lokalisierung, die ID der Softwarelizenz (d. h. die ID der Lizenz, die Sie verlängern) und ob Sie die Lizenz über ein Partnerunternehmen erworben haben oder nicht.

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

   Die Lizenz wird verlängert.

In der Kaspersky Security Center 14 Web Console werden die Benachrichtigungen für eine ablaufende Lizenz entsprechend des folgenden Zeitplans angezeigt:

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

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 14 auf die entsprechende Webseite innerhalb der Kaspersky-Website weiter, wo Sie mehr über diese Lösung erfahren. Jede Produktseite ermöglicht es Ihnen, mit dem Kauf fortzufahren oder enthält Anweisungen zum Kaufprozess.

Im Abschnitt **MARKETPLACE** können Sie die Lösungen von Kaspersky anhand der folgenden Kriterien filtern:

- Anzahl der Geräte (Endpunkte, Server und andere Arten von Assets), die Sie schützen möchten:
  - 50-250

- 250-1000
- Über 1000

- Entwicklungsstufe des Informationssicherheitsteams Ihres Unternehmens:
  - **Foundations**

    Diese Stufe ist typisch für Unternehmen, die nur über ein IT-Team verfügen. Die maximal mögliche Anzahl an Bedrohungen wird automatisch blockiert.
  - **Optimum**

    Diese Stufe ist typisch für Unternehmen, die eine bestimmte IT-Sicherheitsfunktion innerhalb des IT-Teams besitzen. Auf dieser Stufe benötigen Unternehmen Lösungen, die es ihnen ermöglichen, sich einfachen Bedrohungen, und Bedrohungen, die bestehende Präventionsmechanismen umgehen, entgegenzustellen.
  - **Expert**

    Diese Stufe ist typisch für Unternehmen mit komplexen und verteilten IT-Umgebungen. Das IT-Sicherheitsteam ist voll entwickelt oder das Unternehmen verfügt über ein eigenes SOC-Team (Security Operations Center). Die benötigten Lösungen ermöglichen es den Unternehmen, komplexen Bedrohungen und gezielten Angriffen zu begegnen.

- Zu schützende Arten von Assets:
  - **Endpunkte**: Workstations von Mitarbeitern, physische und virtuelle Maschinen, Embedded-Systeme
  - **Server**: physische und virtuelle Server
  - **Cloud**: öffentliche, private oder hybride Cloud-Umgebungen sowie Cloud-Dienste
  - **Netzwerk**: lokales Netzwerk, IT-Infrastruktur
  - **Service**: von Kaspersky angebotene sicherheitsbezogene Dienste

So finden und erwerben Sie eine Business-Lösung von Kaspersky:

1. 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.

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 Maßnahmen

Bevor Sie beginnen, stellen Sie sicher, dass Sie:

- Kaspersky Security Center Administrationsserver installiert haben
- Kaspersky Security Center 14 Web Console installiert haben
- Das Hauptinstallationsszenario für Kaspersky Security Center abgeschlossen haben
- Der Schnellstartassistent wurde abgeschlossen oder die folgenden Richtlinien und Aufgaben wurden manuell in der Administrationsgruppe **Verwaltete Geräte** erstellt:
  - Richtlinie von Kaspersky Endpoint Security
  - Gruppenaufgabe zum Update von Kaspersky Endpoint Security
  - Richtlinie für den Administrationsagenten

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. Diese beiden Methoden können auch kombiniert werden.

2. **Aufgaben zur Remote-Verwaltung von Kaspersky-Programmen konfigurieren**

   Überprüfen Sie die mit dem Schnellstartassistenten erstellten Aufgaben und passen Sie sie bei Bedarf noch feiner an.

   Anleitungen: Gruppenaufgabe für das Update von Kaspersky Endpoint Security einrichten.

   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.

Benutzerzentrierte 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

Nach Abschluss dieses Szenarios werden die Programme gemäß den von Ihnen festgelegten Richtlinien und Richtlinienprofilen auf allen verwalteten Geräten konfiguriert.

Erforderliche Maßnahmen

Bevor Sie beginnen, stellen Sie sicher, dass Sie den Kaspersky Security Center Administrationsserver und Kaspersky Security Center 14 Web Console installiert haben. Sie sollten zusätzlich auch die benutzerorientierte Sicherheitsverwaltung als Alternative oder als zusätzliche Option zur geräteorientierten Herangehensweise in Betracht ziehen. Erfahren Sie mehr über die beiden Verwaltungsmethoden.

Schritte

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 eine Standardrichtlinie für Kaspersky Endpoint Security für Linux. Wenn Sie den Konfigurationsvorgang mithilfe dieses Assistenten abgeschlossen haben, müssen Sie keine neue Richtlinie für dieses Programm erstellen.

   Wenn Sie eine hierarchische Struktur aus mehreren Administrationsservern und/oder Administrationsgruppen haben, erben die sekundären Administrationsserver und die untergeordneten Administrationsgruppen standardmäßig die Richtlinien des primären Administrationsservers. Sie können die Vererbung an die untergeordneten Gruppen und an den sekundären Administrationsserver erzwingen, um Änderungen an den durch die Richtlinie höherer Ebene festgelegten Einstellungen zu verhindern. Wenn Sie möchten, dass nur bestimmte Einstellungen zwangsweise vererbt werden, können Sie diese in der Richtlinie höherer Ebene sperren. Die übrigen, nicht gesperrten Einstellungen können in den Richtlinien niedriger Ebene geändert werden. Dank der erstellten Hierarchie aus Richtlinien können Sie die Geräte in den Administrationsgruppen optimal verwalten.

   Anleitung: Richtlinie erstellen

2. **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 es, verschiedene Richtlinienprofile auf Geräte anzuwenden, die eine bestimmte Hardware-Konfiguration besitzen oder mit bestimmten Tags markiert sind. Verwenden Sie Tags, um Geräte anhand bestimmter Kriterien zu filtern. So können Sie z. B. das Tag *CentOS* erstellen, es allen Geräten mit einem CentOS-Betriebssystem zuweisen und dieses Tag dann als Bedingung zur Aktivierung eines Richtlinienprofils festlegen. Als Ergebnis werden alle Kaspersky-Programme, die auf CentOS-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**

   Standardmäßig synchronisiert Kaspersky Security Center den Administrationsserver automatisch alle 15 Minuten 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 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.

Erforderliche Maßnahmen

Bevor Sie beginnen, stellen Sie sicher, dass Sie den Kaspersky Security Center Administrationsserver und Kaspersky Security Center 14 Web Console erfolgreich installiert und das Hauptbereitstellungsszenario abgeschlossen haben. 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 eine Standardrichtlinie für Kaspersky Endpoint Security. Wenn Sie den Konfigurationsvorgang mithilfe dieses Assistenten abgeschlossen haben, müssen Sie keine neue Richtlinie für dieses Programm erstellen.

   Wenn Sie eine hierarchische Struktur aus mehreren Administrationsservern und/oder Administrationsgruppen haben, erben die sekundären Administrationsserver und die untergeordneten Administrationsgruppen standardmäßig die Richtlinien des primären Administrationsservers. Sie können die Vererbung an die untergeordneten Gruppen und an den sekundären Administrationsserver erzwingen, um Änderungen an den durch die Richtlinie höherer Ebene festgelegten Einstellungen zu verhindern. Wenn Sie möchten, dass nur bestimmte Einstellungen zwangsweise vererbt werden, können Sie diese in der Richtlinie höherer Ebene sperren. Die übrigen, nicht gesperrten Einstellungen können in den Richtlinien niedriger Ebene geändert werden. Dank der erstellten Hierarchie aus Richtlinien können Sie die Geräte in den Administrationsgruppen optimal verwalten.

   Anleitung: Richtlinie erstellen

2. **Gerätebenutzer angeben**

   Weisen Sie die verwalteten Geräte den entsprechenden Benutzern zu.

   Anleitung: Festlegen eines Benutzers als Gerätebesitzer

3. **Typische Benutzerrollen in Ihrem Unternehmen festlegen**

   Überlegen Sie, in welchen unterschiedlichen Bereichen die Mitarbeiter Ihres Unternehmens tätig sind. Teilen Sie alle Mitarbeiter nach ihren Rollen ein. Sie können sie z. B. nach Abteilungen, Berufen oder Positionen unterteilen. Anschließend müssen Sie für jede Gruppe eine Benutzerrolle erstellen. Bedenken Sie, dass jede Benutzerrolle ihr eigenes Richtlinienprofil mit rollenspezifischen 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**

   Standardmäßig synchronisiert Kaspersky Security Center den Administrationsserver automatisch alle 15 Minuten 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 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 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.

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.

Allgemein

Auf dieser Registerkarte können Sie den Richtlinienstatus ändern und die Vererbung der Richtlinieneinstellungen anpassen:

- Im Block **Richtlinienstatus** können Sie einen der Richtlinienmodi auswählen:

- **Aktive Richtlinie**

  Bei Auswahl dieser Option wird die Richtlinie aktiv.

  Diese Variante ist standardmäßig ausgewählt.

- **Inaktive Richtlinie**

  Bei Auswahl dieser Option wird die Richtlinie inaktiv, aber im Ordner **Richtlinien** gespeichert. Bei Bedarf kann die Richtlinie aktiviert werden.

- In der Einstellungsgruppe **Einstellungen erben** können Sie Einstellungen für die Vererbung der Richtlinie anpassen:

  - **Einstellungen aus übergeordneter Richtlinie erben**

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

    Diese Option ist standardmäßig aktiviert.

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

    Ist diese Option aktiviert, so werden die folgenden Aktionen ausgeführt, nachdem die Richtlinienänderungen übernommen wurden:

    - Einstellungen der Richtlinie werden in die Tochter-Richtlinien, d.h. in die Richtlinien der eingebetteten Administrationsgruppen, verbreitet.
    - Im Block **Einstellungen erben** des Abschnitts **Allgemein** im Eigenschaftenfenster aller untergeordneten Richtlinien wird die Option **Einstellungen aus Richtlinie der höheren Ebene erben** automatisch aktiviert.

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

    Diese Option ist standardmäßig deaktiviert.

Konfiguration von Ereignissen

Auf dieser Registerkarte können Sie die Ereignisprotokollierung und die Benachrichtigung über Ereignisse konfigurieren. Ereignisse werden anhand der Ereigniskategorie in die folgenden Abschnitte auf der Registerkarte **Konfiguration von Ereignissen** aufgeteilt:

- **Funktionsfehler**
- **Warnung**
- **Information**

Jeder Abschnitt enthält eine Liste mit Ereignistypen und der Standard-Speicherdauer des Ereignisses auf dem Administrationsserver (in Tagen). Nachdem Sie den Ereignistyps angeklickt haben, können Sie die Eigenschaften für die Protokollierung und die Benachrichtigung über die aus der Liste ausgewählten Ereignisse festgelegt werden. Standardmäßig werden die allgemeinen Benachrichtigungseinstellungen, die für den gesamten Administrationsserver festgelegt wurden, für alle Ereignistypen verwendet. Bestimmte Einstellungen können jedoch für die gewünschten Ereignistypen angepasst werden.

Sie können beispielsweise im Abschnitt **Warnung** den Ereignistyp **Es ist ein Vorfall aufgetreten** konfigurieren. Solche Ereignisse können beispielsweise eintreten, wenn der freie Speicherplatz eines Verteilungspunkts weniger als 2 GB beträgt (es sind mindestens 4 GB erforderlich, um Programme remote zu installieren und Updates herunterzuladen). Um das Ereignis **Es ist ein Vorfall aufgetreten** zu konfigurieren, klicken Sie es an und legen Sie fest, wo die aufgetretenen Ereignisse gespeichert werden sollen und wie über sie benachrichtigt werden soll.

Wenn der Administrationsagent einen Vorfall entdeckt hat, können Sie diesen Vorfall mithilfe der Einstellungen eines verwalteten Geräts verwalten.

Programmeinstellungen

Einstellungen

Im Abschnitt **Einstellungen** können Sie die Richtlinieneinstellungen des Administrationsagenten anpassen:

- **Maximale Größe der Ereigniswarteschlange (MB)**

  In diesem Feld können Sie den maximalen Speicherplatz eingeben, welchen die Ereigniswarteschlange auf dem Laufwerk einnehmen kann.

  Standardmäßig ist der Wert auf 2 MB eingestellt.

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

  Der Administrationsagent, der auf einem verwalteten Gerät installiert ist, überträgt Informationen über die angewendete Sicherheitsanwendungs-Richtlinie an die Sicherheitsanwendung (z. B. Kaspersky Endpoint Security für Linux). 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.

Datenverwaltung

Im Abschnitt **Datenverwaltung** können Sie die Objekttypen auswählen, deren Daten vom Administrationsagenten an den Administrationsserver übertragen werden sollen. Wenn das Ändern der in diesem Abschnitt angegebenen Einstellungen in der Richtlinie des Administrationsagenten unterbunden ist, können Sie diese Einstellungen nicht ändern.

- Details zu installierten Programmen

  Ist diese Option aktiviert, werden auf den Administrationsserver Informationen über die auf den Client-Geräten installierten Programme übertragen.

  Diese Option ist standardmäßig aktiviert.

- Informationen über die Hardware-Inventur

  Der auf einem Gerät installierte Administrationsagent sendet Informationen über die Geräte-Hardware an den Administrationsserver. Sie können die Hardware-Details in den Geräteeigenschaften anzeigen.

Netzwerk

Der Abschnitt **Netzwerk** enthält drei Unterabschnitte:

- **Konnektivität**
- **Verbindungsprofile**
- **Zeitplan der Verbindung**

Im Unterabschnitt **Konnektivität** können Sie die Einstellungen für die Verbindung zum Administrationsserver anpassen, die Nutzung eines UDP-Ports aktivieren und die Nummer des UDP-Ports festlegen.

- In der Einstellungsgruppe **Mit dem Administrationsserver verbinden** können Sie die Verbindungseinstellungen für den Administrationsserver anpassen und das Synchronisierungsintervall der Client-Geräte mit dem Administrationsserver festlegen:

  - Synchronisierungsintervall (Min.)

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

    Bei einem Synchronisierungsintervall kleiner als 15 Minuten, wird die Synchronisierung alle 15 Minuten durchgeführt. Bei einem Synchronisierungsintervall größer gleich 15 Minuten, wird die Synchronisierung entsprechend des angegebenen Synchronisierungsintervalls durchgeführt.

  - Netzwerkverkehr komprimieren

Aktivieren Sie diese Option, um die Geschwindigkeit der Datenübertragung durch den Administrationsagenten zu steigern, das Datenvolumen zu komprimieren und die Belastung für den Administrationsserver zu reduzieren.

Die CPU-Auslastung des Client-Computers kann ansteigen.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

- SSL-Verbindung verwenden

  Wenn diese Option aktiviert ist, erfolgt die Verbindung zum Administrationsserver über einen gesicherten Port mit SSL-Protokoll.

  Diese Option ist standardmäßig aktiviert.

- Verbindungs-Gateway auf 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 ist Portnummer 15000 angegeben.

  Für die Eingabe wird das Dezimalformat verwendet.

Im Unterabschnitt **Verbindungsprofile** des Abschnitts **Netzwerk** können Sie die Einstellungen des Netzwerkstandortes festlegen und den Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist. Die Einstellungen im Abschnitt **Verbindungsprofile** sind nur auf Geräten verfügbar, die unter Windows laufen:

- Einstellungen des Netzwerkstandorts

  Die Einstellungen des Netzwerkspeicherorts bestimmen die Merkmale des Netzwerks, mit dem das Client-Gerät verbunden ist, und legen die Regeln für den Wechsel des Administrationsagenten von einem Administrationsserver-Verbindungsprofil zu einem anderen fest (im Falle sich ändernder Merkmale des Netzwerks).

- Verbindungsprofile des Administrationsservers

Verbindungsprofile werden nur für Windows-Geräte unterstützt. Die Verwendung dieser Option wird nicht empfohlen.

Sie können ein Profil für die Verbindung des Administrationsagenten mit dem Administrationsserver anzeigen und hinzufügen. In diesem Abschnitt können ferner die Umschaltregeln des Administrationsagenten auf andere Administrationsserver im Fall des Auftretens folgender Ereignisse festgelegt werden:

- Verbindung des Client-Geräts mit einem anderen lokalen Netzwerk.
- Trennung der Verbindung des Geräts vom lokalen Unternehmensnetzwerk.
- Änderung der Verbindungs-Gateway-Adresse oder der Adresse des DNS-Servers.

Da in der Einstellungsgruppe **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.

- **Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist**

  Wenn diese Option aktiviert ist, werden die auf dem Client-Gerät installierten Programme bei einer Verbindung über dieses Profil für Geräte, die sich im Modus für mobile Benutzer befinden, Richtlinienprofile und mobile Richtlinien verwenden. Wurde für das Programm keine Richtlinie für mobile Benutzer definiert, verwendet das Programm die aktive Richtlinie.

  Wenn diese Option deaktiviert ist, wenden die Anwendungen die aktiven Richtlinien an.

  Diese Option ist standardmäßig deaktiviert.

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. Sie können die folgenden Optionen verwenden, um die Abfrage zu aktivieren und ihre Häufigkeit festzulegen:

- **Zeroconf**

  Wenn diese Option aktiviert ist, fragt der Verteilungspunkt das Netzwerk mit IPv6-Geräten unter Verwendung von Zero-configuration Networking (auch als *Zeroconf* bezeichnet) automatisch ab. In diesem Fall werden aktivierte IP-Bereichsabfragen ignoriert, da der Verteilungspunkt das gesamte Netzwerk abfragt.

  Um Zeroconf verwenden zu können, müssen die folgenden Bedingungen erfüllt sein:

  - Der Verteilungspunkt muss unter Linux laufen.
  - Sie müssen auf dem Verteilungspunkt das Tool "avahi-browse" installieren.

  Wenn diese Option deaktiviert ist, fragt der Verteilungspunkt Netzwerke mit IPv6-Geräten nicht ab.

  Diese Option ist standardmäßig deaktiviert.

- **IP-Bereiche**

  Wenn diese Option aktiviert ist, fragt der Administrationsserver die IP-Bereiche automatisch gemäß dem Zeitplan ab, den Sie über den Link **Abfragezeitplan festlegen** eingerichtet haben.

  Wenn diese Option deaktiviert ist, fragt der Administrationsserver keine IP-Bereiche ab.

  Das Intervall der Abfrage des IP-Bereichs kann für Versionen des Administrationsagenten bis Version 10.2 im Feld **Abfrageintervall (Min.)** eingestellt werden. Der Abschnitt ist verfügbar, wenn die Option aktiviert ist.

  Diese Option ist standardmäßig deaktiviert.

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 deaktiviert.

- **Benutzername**

- **Kennwort**

Updates (Verteilungspunkte)

Sie können die Funktion zum Download von diff-Dateien im Abschnitt **Updates (Verteilungspunkte)** aktivieren, damit die Verteilungspunkte die Updates in Form von diff-Dateien von den Kaspersky-Update-Servern erhalten.

Revisionsverlauf

Auf dieser Registerkarte können Sie eine Liste mit Revisionen der Richtlinie anzeigen und bei Bedarf ein Rollback der Änderungen an der Richtlinie vornehmen.

Die Priorität der Verschiebungsregeln für Geräte ändern

Die Regeln für das Verschieben von Geräten haben Prioritäten.

Um die Priorität einer Regel zum Verschieben zu erhöhen oder zu verringern,

verschieben Sie die Regel in der Liste mit der Maus nach oben bzw. unten.

Aufgaben

In diesem Abschnitt werden Aufgaben beschrieben, die von Kaspersky Security Center verwendet werden.

Über Aufgaben

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

Aufgaben für ein bestimmtes Programm können mithilfe von Kaspersky Security Center 14 Web Console nur dann erstellt werden, wenn das Verwaltungs-Plug-in für dieses Programm auf dem Server von Kaspersky Security Center 14 Web Console installiert ist.

Aufgaben können auf dem Administrationsserver und auf Geräten ausgeführt werden.

Zu den Aufgaben, die auf dem Administrationsserver ausgeführt werden, gehören:

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

- Datenbank bedienen

Die folgenden Typen von Aufgaben werden auf Geräten ausgeführt:

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

  Lokale Aufgaben können entweder vom Administrator über Kaspersky Security Center 14 Web Console geändert werden oder vom Benutzer eines Remote-Gerätes (beispielsweise über die Benutzeroberfläche einer Sicherheits-App). Wenn eine lokale Aufgabe gleichzeitig sowohl vom Administrator als auch vom Benutzer auf dem verwalteten Gerät geändert wurde, treten jene Änderungen in Kraft, die vom Administrator mit höherer Priorität ausgeführt wurden.

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

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

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

Sie können für jedes Programm eine beliebige Anzahl von Gruppenaufgaben, globalen Aufgaben oder lokalen Aufgaben erstellen.

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

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

Ausführungsergebnisse von Aufgaben werden im Betriebssystem-Ereignisprotokolle auf jedem Gerät, im Betriebssystem-Ereignisprotokoll des Administrationsservers 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 Gerätes können Sie eine IP-Adresse (oder einen IP-Bereich) oder einen 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 zum Hinzufügen von Aufgaben 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.

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 **Benutzerkonto** oder durch Anklicken der Schaltfläche **Ergebnis** überprüfen.

Aufgabenliste anzeigen

Sie können die Liste der Aufgaben anzeigen, die in Kaspersky Security Center Linux erstellt wurden.

Um die Liste der Aufgaben anzuzeigen:

Gehen Sie zu **GERÄTE → AUFGABEN**.

Die Aufgabenliste wird angezeigt. Die Aufgaben sind nach den Namen der Programme gruppiert, auf die sie sich beziehen. Beispielsweise bezieht sich die Aufgabe *Remote-Installation eines Programms* auf den Administrationsserver, und die Aufgabe *Update* bezieht sich auf den Administrationsagenten.

Um die Eigenschaften einer Aufgabe anzuzeigen,

Klicken Sie auf den Namen der Aufgabe.

Das Fenster mit den Aufgabeneigenschaften enthält mehrere benannte Registerkarten. Zum Beispiel wird der **Aufgabentyp** auf der Registerkarte **Allgemein** angezeigt und der Aufgabenzeitplan auf der Registerkarte **Zeitplan**.

Allgemeine Aufgabeneinstellungen

Dieser Abschnitt enthält die Einstellungen, die Sie für Aufgaben anzeigen und angeben können.

Einstellungen, die während der Aufgabenerstellung festgelegt werden

Sie können beim Erstellen einer Aufgabe die folgenden Einstellungen festlegen. Einige dieser Einstellungen können auch in den Eigenschaften der erstellten Aufgabe geändert werden.

- Neustart-Einstellungen des Betriebssystems:
  - **Gerät nicht neu starten**

    Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. 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.

- 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.

- Zeitplaneinstellungen für Aufgaben:

  - Start nach Zeitplan

    Legen Sie den Zeitplan fest, nach dem die Aufgabe ausgeführt werden soll, und passen Sie den ausgewählten Zeitplan an.

    - Alle n Stunden

      Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

      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.

    - Alle n Minuten

Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

- **Täglich (Sommerzeit wird nicht unterstützt)**

  Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. In diesem Zeitplan wird die Einhaltung der Sommerzeit nicht unterstützt. Das bedeutet, wenn die Uhren zu Beginn oder am Ende der Sommerzeit eine Stunde vor- oder zurückgestellt werden, ändert sich die tatsächliche Startzeit der Aufgabe nicht.

  Es wird nicht empfohlen, diesen Zeitplan zu verwenden. Er wird für die Abwärtskompatibilität von Kaspersky Security Center Linux benötigt.

  Standardmäßig wird die Aufgabe jeden Tag zur aktuellen Systemzeit gestartet.

- **Wöchentlich**

  Die Aufgabe wird jede Woche am festgelegten Tag und zur festgelegten Uhrzeit ausgeführt.

- **Nach Wochentagen**

  Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

  Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich**

  Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

  In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

  Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Manuell**

  Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

  Diese Option ist standardmäßig aktiviert.

- **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**

Die Aufgabe wird gestartet, nachdem Updates in die Datenverwaltung heruntergeladen wurden. Sie können diesen Zeitplan beispielsweise die *Update*-Aufgabe verwenden.

- **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.

- **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.

- Geräte, denen die Aufgabe zugewiesen wird:

  - **Geräte auswählen, die vom Administrationsserver im Netzwerk gefunden wurden**

Die Aufgabe wird einer Reihe von Geräten zugewiesen. In dieser Reihe von Geräten können Sie sowohl Geräte aus den Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.

Sie können diese Option beispielsweise für eine Aufgabe zur Installation des Administrationsagenten auf nicht zugeordneten Geräten verwenden.

- **Geräteadressen manuell festlegen oder aus einer Liste importieren**

  Sie können DNS-Namen, IP-Adressen und IP-Subnetze der Geräte angeben, denen die 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 zur Geräteauswahl festlegen**

  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.

- **Aufgabe der 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.

- 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 angeben**

    Füllen Sie die Felder **Benutzerkonto** und **Kennwort** aus. Geben Sie hier die Details für das Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll. Das Benutzerkonto muss über die für diese Aufgabe erforderlichen Rechte verfügen.

  - **Benutzerkonto**

    Benutzerkonto, unter dessen Namen die Aufgabe ausgeführt wird.

  - **Kennwort**

Kennwort des Benutzerkontos, unter dessen Namen die Aufgabe gestartet wird.

Einstellungen, die nach der Aufgabenerstellung festgelegt werden

Sie können die folgenden Einstellungen erst festlegen, nachdem eine Aufgabe erstellt wurde.

- Einstellungen der Gruppenaufgabe:
  - **Auf Untergruppen verteilen**

    Diese Option ist nur in den Einstellungen der Gruppenaufgaben verfügbar.

    Wenn diese Option aktiviert ist, umfasst der Gültigkeitsbereich der Aufgabe die folgenden Objekte:

    - Die Administrationsgruppe, die Sie beim Erstellen der Aufgabe ausgewählt haben.
    - Die Administrationsgruppen, die der ausgewählten Administrationsgruppe entsprechend der Gruppenhierarchie auf beliebiger Ebene untergeordnet sind.

    Wenn diese Option deaktiviert ist, umfasst der Gültigkeitsbereich der Aufgabe nur die Administrationsgruppe, die Sie beim Erstellen der Aufgabe ausgewählt haben.

    Diese Option ist standardmäßig aktiviert.

  - **An sekundäre und virtuelle Administrationsserver verteilen**

    Wenn diese Option aktiviert ist, wird die Aufgabe, die auf dem primären Administrationsserver wirksam ist, auch auf den sekundären Administrationsservern (einschließlich virtuellen) angewendet. Wenn auf dem sekundären Administrationsserver bereits eine Aufgabe des gleichen Typs existiert, werden auf dem sekundären Administrationsserver beide Aufgaben angewendet – die bestehende und die vom primären Administrationsserver übernommene.

    Diese Option ist nur verfügbar, wenn die Option **Auf Untergruppen verteilen** aktiviert ist.

    Diese Option ist standardmäßig deaktiviert.

- Erweiterte Zeitplaneinstellungen:
  - **Gerät vor dem Start der Aufgabe über Wake-On-LAN aktivieren (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 **Gerät nach Beendigung der Aufgabe herunterfahren**. Die Option befindet sich im selben Fenster.

    Diese Option ist standardmäßig deaktiviert.

  - **Geräte nach Abschluss der Aufgabe abschalten**

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 Aufgabe länger ausgeführt wird als (Min.)

  Nachdem die festlegte Zeitspanne abgelaufen ist, wird die Aufgabe automatisch angehalten, egal ob sie abgeschlossen ist oder nicht.

  Aktivieren Sie diese Option, wenn Sie Aufgaben, deren Ausführung zu lange dauert, unterbrechen (oder anhalten) möchten.

  Diese Option ist standardmäßig deaktiviert. Die Standardzeit für die Aufgabenausführung beträgt 120 Minuten.

- Benachrichtigungseinstellungen:
  - Block **Ereignisdaten 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

      Programmereignisse, die sich auf die Ausführung der Aufgabe beziehen, werden lokal im Syslog-Ereignisprotokoll jedes Client-Gerätes gespeichert.

      Diese Option ist standardmäßig deaktiviert.

    - Im System-Ereignisprotokoll des Administrationsservers speichern

      Programmereignisse, die sich auf die Ausführung der Aufgabe auf allen Client-Geräten aus dem Aufgabenbereich beziehen, werden zentral im Syslog-Ereignisprotokoll des Betriebssystems des Administrationsservers gespeichert.

      Diese Option ist standardmäßig deaktiviert.

    - Alle Ereignisse speichern

      Wenn diese Option ausgewählt ist, werden alle Ereignisse, die sich auf die Aufgabe beziehen, in den Ereignisprotokollen gespeichert.

    - Ereignisse in Bezug auf Aufgabenfortschritt speichern

Wenn diese Option ausgewählt ist, werden nur Ereignisse, die sich auf die Aufgabenausführung beziehen, in den Ereignisprotokollen gespeichert.

- Nur die Ergebnisse der Aufgabenausführung speichern

  Wenn diese Option ausgewählt ist, werden nur Ereignisse, die sich auf die Ergebnisse der Aufgabenausführung beziehen, in den Ereignisprotokollen gespeichert.

- Den Administrator über Ergebnisse der Aufgabenausführung benachrichtigen

  Sie können die Methoden auswählen, über die Administratoren Benachrichtigungen über Ergebnisse der Aufgabenausführung erhalten: per E-Mail, mit SMS und durch Start einer ausführbaren Datei. Um die Benachrichtigungen zu konfigurieren, klicken Sie auf den Link **Einstellungen**.

  Standardmäßig sind alle Methoden der Zustellung von Benachrichtigungen deaktiviert.

- Nur über Fehler benachrichtigen

  Wenn diese Option aktiviert ist, werden Administratoren nur dann benachrichtigt, wenn die Aufgabenausführung mit einem Fehler beendet wird.

  Wenn diese Option deaktiviert ist, werden Administratoren nach jeder Aufgabenausführung benachrichtigt.

  Diese Option ist standardmäßig aktiviert.

- Sicherheitseinstellungen.

- Einstellungen für den Gültigkeitsbereich der Aufgabe.

  Abhängig davon, wie der Gültigkeitsbereich der Aufgabe bestimmt wird, sind die folgenden Einstellungen verfügbar:

  - Geräte

    Wenn der Gültigkeitsbereich einer Aufgabe durch eine Administrationsgruppe bestimmt wird, können Sie diese Gruppe anzeigen. Hier sind keine Änderungen möglich. Sie können aber **Ausschlüsse vom Gültigkeitsbereich der Aufgabe** festlegen.

    Wenn der Gültigkeitsbereich einer Aufgabe durch eine Liste von Geräten bestimmt wird, können Sie diese Liste ändern, indem Sie Geräte hinzufügen und entfernen.

  - Geräteauswahl

    Sie können die Geräteauswahl ändern, für welche die Aufgabe übernommen wird.

  - Ausschlüsse vom Aufgabengültigkeitsbereich

    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.**

Assistent zum Ändern der Aufgabenkennwörter starten

Für eine nicht lokale Aufgabe können Sie ein Benutzerkonto angeben, unter dem die Aufgabe ausgeführt werden soll. Sie können das Benutzerkonto bei der Aufgabenerstellung oder in den Eigenschaften einer vorhandenen Aufgabe angeben. Wenn das angegebene Benutzerkonto den Sicherheitsvorschriften des Unternehmens unterliegt, müssen Sie das Benutzerkonto-Kennwort möglicherweise von Zeit zu Zeit ändern. Wenn das Benutzerkonto-Kennwort abläuft und Sie ein neues festlegen, müssen Sie das neue gültige Kennwort in den Aufgabeneigenschaften angeben, damit die Aufgaben korrekt starten können.

Mit dem Assistenten zum Ändern der Aufgabenkennwörter können Sie das alte Kennwort in allen Aufgaben, in denen das Benutzerkonto angegeben ist, automatisch durch das neue Kennwort ersetzen. Alternativ können Sie das Kennwort auch manuell in den Eigenschaften der einzelnen Aufgaben ändern.

Um den Assistenten zum Ändern der Aufgabenkennwörter zu starten:

1. Wählen Sie auf der Registerkarte **GERÄTE** die Option **AUFGABEN**.
2. Klicken Sie auf die Schaltfläche **Benutzerkonto-Anmeldedaten für den Aufgabenstart verwalten**.

Folgen Sie den Anweisungen des Assistenten.

Schritt 1. Anmeldedaten angeben

Geben Sie neue Anmeldedaten an, die derzeit in Ihrem System gültig sind. Wenn Sie zum nächsten Schritt des Assistenten wechseln, überprüft Kaspersky Security Center, ob der angegebene Benutzerkonto-Name mit dem Benutzerkonto-Namen in den Eigenschaften der einzelnen nicht lokalen Aufgaben übereinstimmt. Stimmen die Benutzerkonto-Namen überein, so wird das Kennwort in den Aufgabeneigenschaften automatisch durch das neue ersetzt.

Um das neue Konto anzugeben, wählen Sie eine Option aus:

- **Aktuelles Benutzerkonto verwenden**

  Der Assistent verwendet den Namen des Kontos, unter dem Sie derzeit bei Kaspersky Security Center 14 Web Console angemeldet sind. Geben Sie dann manuell das Kontokennwort in dem Feld **Aktuelles Kennwort für die Verwendung in Aufgaben** ein.

- **Anderes Benutzerkonto angeben**

  Geben Sie den Namen des Kontos an, unter dem die Aufgaben gestartet werden sollen. Geben Sie dann das Kontokennwort in dem Feld **Aktuelles Kennwort für die Verwendung in Aufgaben** ein.

Wenn Sie das Feld **Vorheriges Kennwort (optional; wenn Sie es durch das Aktuelle ersetzen wollen)** ausfüllen, ersetzt Kaspersky Security Center das Kennwort nur für jene Aufgaben, in denen sowohl der Benutzerkonto-Name als auch das alte Kennwort gefunden werden. Das Ersetzen erfolgt automatisch. In allen übrigen Fällen müssen Sie eine Aktion auswählen, die beim nächsten Schritt des Assistenten ausgeführt werden soll.

Schritt 2. Aktion auswählen

Wenn Sie beim ersten Schritt des Assistenten das alte Kennwort nicht angegeben haben oder das angegebene alte Kennwort nicht mit den Kennwörtern in den Aufgabeneigenschaften übereinstimmt, müssen Sie eine Aktion auswählen, die für die gefundenen Aufgaben ausgeführt werden soll.

So wählen Sie eine Aktion für eine Aufgabe aus:

1. Aktivieren Sie das Kontrollkästchen neben der Aufgabe, für die Sie eine Aktion wählen möchten.
2. Führen Sie eine der folgenden Optionen aus:
   - Um das Kennwort in den Aufgabeneigenschaften zu entfernen, klicken Sie auf **Anmeldedaten löschen**.

     Die Aufgabe wird so angepasst, dass sie unter dem Standardkonto ausgeführt wird.
   - Um das Kennwort durch das neue zu ersetzen, klicken Sie auf **Die Änderung des Kennworts erzwingen, selbst wenn das alte Kennwort falsch oder nicht angegeben ist**.
   - Um die Kennwortänderung abzubrechen, klicken Sie auf **Es ist keine Aktion ausgewählt**.

Die ausgewählten Aktionen werden angewendet, wenn Sie zum nächsten Schritt des Assistenten gewechselt sind.

Schritt 3. Ergebnisse anzeigen

Zeigen Sie beim letzten Schritt des Assistenten die Ergebnisse die einzelnen gefundenen Aufgaben an. Klicken Sie auf **Fertig stellen**, um den Assistenten abzuschließen.

Auf dem Administrationsserver gespeicherte Ergebnisse der Aufgabenausführung anzeigen

Kaspersky Security Center Linux erlaubt Ihnen, die Ausführungsergebnisse für Gruppenaufgaben, Aufgaben für eine Reihe von Geräten und Aufgaben des Administrationsservers anzuzeigen. Die Ausführungsergebnisse der lokalen Aufgaben können nicht angezeigt werden.

Um sich die Ergebnisse der Aufgabenausführung anzeigen zu lassen, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Allgemein** aus.
2. Öffnen Sie mithilfe des Links **Ergebnisse** das Fenster **Ergebnisse der Aufgabenausführung**.

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. Wählen Sie **GERÄTE → VERWALTETE GERÄTE** aus.
   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 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 aufrechterhalten. 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 folgende Informationen zu den Netzwerkeinstellungen des Client-Gerätes angezeigt:

- **IP-Adresse**

  IP-Adresse des Geräts.

- **Windows-Domäne**

  Arbeitsgruppe, in der das Gerät enthalten ist.

- **DNS-Name**

  Name der DNS-Domäne des Client-Geräts.

- **NetBIOS-Name**

  Name des Client-Gerätes.

System

Im Abschnitt **System** werden Daten zum Betriebssystem angezeigt, das auf dem Client-Gerät installiert ist.

Schutz

Im Abschnitt **Schutz** werden Informationen über den Status des Antiviren-Schutzes auf dem Client-Gerät angezeigt:

- **Gerätestatus**

  Status, der einem Client-Gerät anhand der vom Administrator festgelegten Kriterien seines Antiviren-Schutzstatus 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 Untersuchung auf Viren 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.

Der Status des Geräts wird vom Programm bestimmt

Im Abschnitt **Gerätestatus wird vom Programm bestimmt** werden Daten über den Gerätestatus angezeigt, der durch das auf dem Gerät installierte verwaltete Programm bestimmt wird. Der Gerätestatus kann von dem durch Kaspersky Security Center Linux 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

Im Abschnitt **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

Im Abschnitt **Ereignisse** werden Ereignisse angezeigt, die für das ausgewählte Client-Gerät auf dem Administrationsserver registriert wurden.

Tags

Im Abschnitt **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.

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

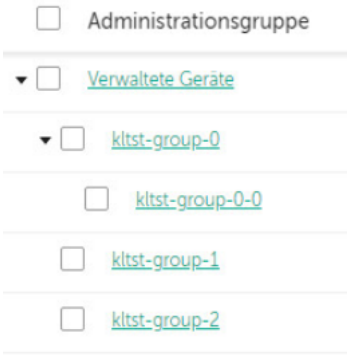
  Mithilfe der Schaltfläche **Eigenschaften** können Sie die Einstellungen der Verteilungspunkte, mit denen das Gerät interagiert, anzeigen und anpassen.

Hardware-Inventur

Im Abschnitt **Hardware-Inventur** finden Sie Informationen zur Hardware, die auf dem Client-Gerät installiert ist.

Administrationsgruppen anlegen

Unmittelbar nach der Installation von Kaspersky Security Center enthält die Hierarchie der Administrationsgruppen nur eine einzige Administrationsgruppe mit dem Namen: **Verwaltete Geräte**. Wenn Sie eine Hierarchie der Administrationsgruppen erstellen, können Sie Geräte, virtuelle Maschinen und untergeordnete Gruppen zur Gruppe **Verwaltete Geräte** hinzufügen (siehe folgende Abbildung).



Hierarchie der Administrationsgruppen erstellen

Um eine Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Gehen Sie zu **GERÄTE** → **GRUPPENHIERARCHIE**.
2. Wählen Sie in der Hierarchie der Administrationsgruppen die Administrationsgruppe aus, welche die neue Administrationsgruppe enthalten soll.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**.
4. Geben Sie im folgenden Fenster **Name der neuen Administrationsgruppe** den Namen der Gruppe ein, und klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

In der Hierarchie der Administrationsgruppen erscheint eine neue Administrationsgruppe mit dem angegebenen Namen.

Um die Struktur der Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Gehen Sie 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.

Verschiebungsregeln für Geräte

Es wird empfohlen, die Verteilung von Geräten auf Administrationsgruppen mithilfe der *Regeln für das Verschieben von Geräten* zu automatisieren. Die Regel zum Verschieben besteht aus drei Hauptteilen: dem Namen, der Ausführungsbedingung (logischer Ausdruck über die Attribute des Geräts) und der Zieladministrationsgruppe. Die Regel verschiebt das Gerät in die Zieladministrationsgruppe, wenn die Attribute des Geräts die Bedingung für die Regelausführung erfüllen.

Die Regeln für das Verschieben von Geräten haben Prioritäten. Der Administrationsserver prüft die Attribute des Geräts auf Übereinstimmung mit der Bedingung für die jeweilige Regelausführung in abnehmender Priorität der Regeln. Wenn die Attribute des Geräts die Bedingungen für die Regelausführung erfüllen, wird das Gerät in die Zielgruppe verschoben und beendet daraufhin die Verarbeitung der Regeln für das betreffende Gerät. Wenn die Attribute des Geräts sofort einigen Regeln entsprechen, wird das Gerät in die Zielgruppe jener Regel verschoben, welche die höchste Priorität hat (in der Liste der Regeln weiter oben steht).

Die zum Geräte verschieben können implizit erstellt werden. Beispielsweise kann in den Eigenschaften des Installationspakets oder der Aufgabe zur Remote-Installation die Administrationsgruppe angegeben werden, in die das Gerät gelangen soll, nachdem darauf der Administrationsagent installiert wurde. Regeln zum Verschieben von Geräten kann der Administrator von Kaspersky Security Center Linux auch explizit im Abschnitt **GERÄTE** → **VERSCHIEBUNGSREGELN** erstellen.

Die Regel zum Verschiebung ist standardmäßig für die einmalige erstmalige Verteilung der Geräte auf die Administrationsgruppen vorgesehen. Die Regel verschiebt die Geräte, die sich in der Gruppe für nicht zugeordnete Geräte befinden, nur einmal. Wenn ein Gerät von dieser Regel einmal verschoben wurde, wird es nicht nochmals von der Regel verschoben, selbst wenn das Gerät manuell erneut in die Gruppe für nicht zugeordnete Geräte verschoben wird. Dies ist die empfohlene Art der Nutzung der Regeln zum Verschieben.

Es können Geräte verschoben werden, die sich bereits in Administrationsgruppen befinden. Dazu muss in den Eigenschaften der Regel das Kontrollkästchen **Nur Geräte verschieben, die keiner Administrationsgruppe angehören** deaktiviert werden.

Durch die Existenz von Regeln zum Verschieben, die auf Geräte gelten, die bereits in die Administrationsgruppen verschoben wurden, steigt die Belastung auf dem Administrationsserver erheblich.

Es kann eine Regel zum Verschieben erstellt werden, die auf einem Gerät mehrfach ausgeführt werden kann.

Es wird dringend empfohlen, Szenarien zu vermeiden, bei denen ein verwaltetes Gerät mehrfach aus einer Gruppe in eine andere verschoben wird (z. B. um eine besondere Richtlinie auf das Gerät anzuwenden, eine spezielle Gruppenaufgabe zu starten oder das Gerät über einen bestimmten Verteilungspunkt zu aktualisieren).

Solche Szenarien werden nicht unterstützt, da sie die Belastung des Administrationsservers und den Datenverkehr in extremem Ausmaß erhöhen. Diese Szenarien stehen ferner in Konflikt mit den Betriebsprinzipien von Kaspersky Security Center Linux (insbesondere im Bereich von Zugriffsrechen, Ereignissen und Berichten). Es müssen andere Lösungen gesucht werden, zum Beispiel durch Verwendung der Richtlinienprofile, der Aufgaben für Geräteauswahlen, die Zuweisung von Administrationsagenten entsprechend dem Standardszenario und so weiter.

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 zur Registerkarte **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.

- **Ausführung der Regel**

  Sie können eine der folgenden Varianten auswählen:

  - Wird einmal pro Gerät ausgeführt.

    Die Regel wird für jedes Gerät, das Ihren Kriterien entspricht, einmal ausgeführt.

  - Wird einmal pro Gerät ausgeführt, dann 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 anwenden.

    Die Regel wird gemäß einem Zeitplan angewendet, der automatisch vom Administrationsserver festgelegt wird (in der Regel alle paar Stunden).

- **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.

- **Regel aktivieren**

  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.

4. Definieren Sie auf der Registerkarte **Regelbedingungen** mindestens ein Kriterium, nach dem die Geräte in eine Administrationsgruppe verschoben werden.

5. Klicken Sie auf die Schaltfläche **Speichern**.

Die Verschiebungsregel wird erstellt. Sie wird in der Liste der Verschiebungsregeln angezeigt. Je höher ihre Position in der Liste ist, desto höher ist die Priorität der Regel. 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. Wechseln Sie im Hauptmenü zur Registerkarte **GERÄTE** → **VERSCHIEBUNGSREGELN**.

   Alternativ können Sie **GERÄTESUCHE UND SOFTWAREVERTEILUNG** → **SOFTWAREVERTEILUNG UND ZUWEISUNG** und anschließend im Menü **VERSCHIEBUNGSREGELN** auswählen.

   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.

   - **Ausführung der Regel**

     Sie können eine der folgenden Varianten auswählen:

     - Wird einmal pro Gerät ausgeführt.

       Die Regel wird für jedes Gerät, das Ihren Kriterien entspricht, einmal ausgeführt.

     - Wird einmal pro Gerät ausgeführt, dann 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 anwenden.

       Die Regel wird gemäß einem Zeitplan angewendet, der automatisch vom Administrationsserver festgelegt wird (in der Regel alle paar Stunden).

   - **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.

- **Regel aktivieren**

  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.

5. Definieren Sie auf der Registerkarte **Regelbedingungen** mindestens ein Kriterium für die Geräte, die automatisch verschoben werden sollen.
6. Klicken Sie auf die Schaltfläche **Speichern**.

Die neue Verschiebungsregel wird erstellt. Sie wird in der Liste der Verschiebungsregeln angezeigt.

Bedingungen für Verschiebungsregeln für Geräte

Wenn Sie eine Regel erstellen oder kopieren, um Client-Geräte in Administrationsgruppen zu verschieben, geben Sie auf der Registerkarte **Regelbedingungen** die Bedingungen zum Verschieben der Geräte an. Um festzulegen, welche Geräte verschoben werden sollen, können Sie die folgenden Kriterien verwenden:

- Den Client-Geräten zugewiesene Tags.
- Netzwerkparameter. Beispielsweise können Sie Geräte mit IP-Adressen aus einem bestimmten Bereich verschieben.
- Verwaltete Programme, die auf Client-Geräten installiert sind, z. B. Administrationsagent oder Administrationsserver.
- Client-Geräte, die virtuelle Maschinen sind.

Nachfolgend finden Sie die Beschreibung, wie Sie diese Informationen in Verschiebungsregeln für Geräte angeben.

Wenn Sie in der Regel mehrere Bedingungen, werden alle mittels logischem UND-Operator verknüpft und alle Bedingungen gelten gleichzeitig. Wenn Sie gar keine Optionen auswählen oder einige Felder leer lassen, gelten diese Bedingungen nicht.

Registerkarte Tags

Auf dieser Registerkarte können Sie eine Verschiebungsregel für Geräte basierend auf Geräte-Tags anpassen, die den Beschreibungen der Client-Geräte zuvor hinzugefügt wurden. Wählen Sie dazu die erforderlichen Tags aus. Darüber hinaus können Sie die folgenden Optionen aktivieren:

- **Auf Geräte ohne angegebene Tags anwenden**

Wenn diese Option aktiviert ist, werden alle Geräte mit den angegebenen Tags von einer Verschiebungsregel ausgeschlossen. Wenn diese Option deaktiviert ist, gilt die Verschiebungsregel für Geräte mit allen ausgewählten Tags.

Diese Option ist standardmäßig deaktiviert.

- Anwenden, wenn mindestens eins der ausgewählten Tags zutrifft

  Wenn diese Option aktiviert ist, gilt eine Verschiebungsregel für Client-Geräte mit mindestens einem der ausgewählten Tags. Wenn diese Option deaktiviert ist, gilt die Verschiebungsregel für Geräte mit allen ausgewählten Tags.

  Diese Option ist standardmäßig deaktiviert.

Registerkarte Netzwerk

Auf dieser Registerkarte können Sie die Netzwerkdaten von Geräten angeben, die eine Verschiebungsregel für Geräte berücksichtigt:

- DNS-Name des Geräts

  Name der DNS-Domänen des Client-Geräts, das Sie verschieben möchten. Füllen Sie dieses Feld aus, wenn Ihr Netzwerk einen DNS-Server enthält.

- DNS-Domäne

  Eine Verschiebungsregel gilt für alle Geräte, die im angegebenen primären DNS-Suffix enthalten sind. Füllen Sie dieses Feld aus, wenn Ihr Netzwerk einen DNS-Server enthält.

- IP-Bereich

  Wenn diese Option aktiviert ist, können Sie in den Eingabefeldern die erste und die letzte IP-Adresse des Bereichs eingeben, zu dem die betreffenden Geräte gehören sollen.

  Diese Option ist standardmäßig deaktiviert.

- IP-Adresse für die Verbindung mit dem Administrationsserver

  Wenn diese Option aktiviert ist, können Sie die IP-Adressen festlegen, über die Client-Geräte mit dem Administrationsserver verbunden werden. Geben Sie dazu den IP-Bereich an, der alle notwendigen IP-Adressen enthält.

  Diese Option ist standardmäßig deaktiviert.

- Verbindungsprofil wurde geändert

Wählen Sie eine der folgenden Werte aus:

- **Ja**. Eine Verschiebungsregel gilt nur für Client-Geräte mit einem geänderten Verbindungsprofil.
- **Nein**. Die Verschiebungsregel gilt nur für Client-Geräte, deren Verbindungsprofile sich nicht geändert haben.
- **Es wurde kein Wert gewählt**. Die Bedingung trifft nicht zu.

- 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.

Registerkarte Programme

Auf dieser Registerkarte können Sie eine Regel zum Verschieben von Geräten basierend auf den verwalteten Programmen und Betriebssystemen konfigurieren, die auf Client-Geräten installiert sind:

- Administrationsagent ist installiert

Wählen Sie eine der folgenden Werte aus:

- **Ja**. Eine Verschiebungsregel gilt nur für Client-Geräte, auf denen der Administrationsagent installiert ist.
- **Nein**. Die Verschiebungsregel gilt nur für Client-Geräte, auf denen der Administrationsagent nicht installiert ist.
- **Es wurde kein Wert gewählt**. Die Bedingung trifft nicht zu.

- Programme

Geben Sie an, welche verwalteten Programme auf Client-Gerät installiert sein müssen, damit für diese Geräte eine Verschiebungsregel gilt. Sie können beispielsweise **Kaspersky Security Center 14 Administrationsagent** oder **Kaspersky Security Center 14 Administrationsserver** angeben.

Wenn Sie keine verwaltetes Programm auswählen, trifft die Bedingung nicht zu.

- Version des Betriebssystems

Sie können Client-Geräte basierend auf deren Betriebssystemversionen auswählen. Geben Sie dazu Betriebssysteme an, die auf den Client-Geräten installiert sein müssen. Als Ergebnis gilt eine Verschiebungsregeln für die Client-Geräte mit den ausgewählten Betriebssystemen.

Wenn Sie diese Option nicht aktivieren, trifft die Bedingung nicht zu. Die Option ist standardmäßig deaktiviert.

- **Bitzahl des Betriebssystems**

  Sie können Client-Geräte anhand der Bitanzahl des Betriebssystems auswählen. Im Block **Bitzahl des Betriebssystems** können Sie einen der folgenden Werte auswählen:

  - **Unbekannt**
  - **x86**
  - **AMD64**
  - **IA64**

  So überprüfen Sie die Bitanzahl des Betriebssystems der Client-Geräte:

  1. Wechseln Sie im Hauptmenü zum Abschnitt **GERÄTE** → **VERWALTETE GERÄTE**.
  2. Klicken Sie auf die Schaltfläche **Columns settings** ( ) auf der rechten Seite.
  3. Aktivieren Sie die Option **Bitzahl des Betriebssystems** und klicken Sie anschließend auf die Schaltfläche **Speichern**.

     Danach wird die Bitanzahl des Betriebssystems für jedes verwaltete Gerät angezeigt.

- **Service Pack-Version des Betriebssystems**

  In diesem Feld können Sie die 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.

- **Benutzerzertifikat**

  Wählen Sie eine der folgenden Werte aus:

  - **Installiert**. Eine Verschiebungsregel gilt nur für mobile Geräte mit einem mobilen Zertifikat.
  - **Nicht installiert**. Die Verschiebungsregel gilt nur für mobile Geräte ohne mobiles Zertifikat.
  - **Es wurde kein Wert gewählt**. Die Bedingung trifft nicht zu.

- **Build-Version des Betriebssystems**

Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Versionsnummer haben muss. Sie können auch eine Verschiebungsregel für Geräte für alle Versionsnummern mit Ausnahme der angegebenen anpassen.

- Releasenummer des Betriebssystems

  Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

  Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Release-Nummer haben muss. Sie können auch eine Verschiebungsregel für Geräte für allen Versionsnummern mit Ausnahme der angegebenen anpassen.

Registerkarte Virtuelle Maschinen

Auf dieser Registerkarte können Sie die Verschiebungsregel für Geräte anpassen, je nachdem, ob die Client-Geräte virtuelle Maschinen sind oder zur Virtual Desktop Infrastructure (VDI) gehören:

- Ist eine virtuelle Maschine

  In der Dropdown-Liste können Sie einen der folgenden Werte auswählen:
  - **Maximale Kapazität des Dienstes wurde überschritten**. Die Bedingung trifft nicht zu.
  - **Nein**. Geräte verschieben, die keine virtuellen Maschinen sind.
  - **Ja**. Geräte verschieben, die virtuellen Maschinen sind.

- **Typ der virtuellen Maschine**

- Gehört zur Virtual Desktop Infrastructure (VDI)

  In der Dropdown-Liste können Sie einen der folgenden Werte auswählen:
  - **Maximale Kapazität des Dienstes wurde überschritten**. Die Bedingung trifft nicht zu.
  - **Nein**. Geräte verschieben, die keine Teil einer VDI sind.
  - **Ja**. Geräte verschieben, die Teil einer VDI sind.

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. Gehen Sie 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 einen Geräte-DNS-Namen 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 in eine Administrationsgruppe

Sie können Geräte aus einer Administrationsgruppe in eine andere oder von der Gruppe nicht zugeordneter Geräte in eine Administrationsgruppe verschieben.

Um eines oder mehrere Geräte zu einer gewählten Administrationsgruppe zu verschieben, gehen Sie wie folgt vor:

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 zu **GERÄTE** → **Gruppen** → **<Gruppenname>** → **VERWALTETE GERÄTE**.

   - Um die Gruppe **NICHT ZUGEORDNETE GERÄTE** zu öffnen, wechseln Sie zu **GERÄTESUCHE UND SOFTWAREVERTEILUNG** → **NICHT ZUGEORDNETE GERÄTE**.

2. Aktivieren Sie die Kontrollkästchen neben den Geräten, die Sie in eine andere Gruppe verschieben möchten.

3. Klicken Sie auf die Schaltfläche **In Gruppe verschieben**.

4. Aktivieren Sie in der Hierarchie der Verwaltungsgruppen das Kontrollkästchen neben der Administrationsgruppe, in welche Sie die ausgewählten Geräte verschieben möchten.

5. Klicken Sie auf die Schaltfläche **Verschieben**.

Die ausgewählten Geräte werden in die gewählte Administrationsgruppe verschoben.

Administrationsserver für Client-Geräte wechseln

Sie können für bestimmte Client-Geräte einen anderen Administrationsserver festlegen. Verwenden Sie dazu die Aufgabe *Administrationsserver wechseln*.

Um einen Administrationsserver, der die Client-Geräte verwaltet, zu wechseln, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zum Administrationsserver her, der die Geräte verwaltet.

2. Erstellen Sie die Aufgabe "Administrationsserver ändern".

   Der Assistent zum Hinzufügen von Aufgaben wird gestartet. Folgen Sie den Anweisungen des Assistenten. Wählen Sie im Fenster **Neue Aufgabe** des Assistenten für das Hinzufügen einer Aufgabe das Programm **Hersteller** und den Aufgabentyp **Administrationsserver wechseln** aus. Geben Sie dann die Geräte an, für die Sie den Administrationsserver ändern möchten:

   - **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 DNS-Namen, IP-Adressen und IP-Subnetze der Geräte angeben, denen die 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.

3. 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.

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 Linux weist jedem verwalteten Gerät einen Status zu. Der jeweilige Status hängt davon ab, ob die vom Benutzer definierten Bedingungen erfüllt sind. Wenn Kaspersky Security Center Linux einem Gerät einen Status zuweist, wird in bestimmten Fällen das Sichtbarkeits-Flag des Gerätes im Netzwerk berücksichtigt (siehe folgende Tabelle). Wenn Kaspersky Security Center Linux ein Gerät innerhalb von zwei Stunden nicht im Netzwerk findet, wird das Sichtbarkeits-Flag des Gerätes auf *Nicht sichtbar* gesetzt.

Es gibt folgende Statusvarianten:

- *Kritisch* oder *Kritisch/Sichtbar*
- *Warnung* oder *Warnung/Sichtbar*
- *OK* oder *OK/Sichtbar*

Die folgende Tabelle enthält die erforderlichen Standardbedingungen, nach denen einem Gerät der Status *Kritisch* oder *Warnung* zugewiesen wird, sowie alle möglichen Werte.

Bedingungen für das Zuweisen der Status an das Gerät

Bedingung	Beschreibung der Bedingung	Mögliche Werte
Es wurde keine Sicherheitsanwendung installiert	Auf dem Gerät ist der Administrationsagent installiert, aber es wurde keine Sicherheitsanwendung installiert.	• Umschalter aktiviert.

		• Umschalter deaktiviert.
Zu viele Viren gefunden	Auf dem Gerät wurden 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 Untersuchung auf Viren liegt lange zurück	Das Gerät ist im Netzwerk sichtbar und eine Sicherheits-App wurde auf dem Gerät installiert, aber die Aufgabe "Untersuchung auf Viren" wurde nicht 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 installiert	Das Gerät ist im Netzwerk sichtbar, aber infolge der Inventarisierung der Software durch den Administrationsagenten wurden auf dem Gerät inkompatible Programme gefunden.	• Umschalter deaktiviert. • Umschalter aktiviert.
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.
Es wurden	Auf dem Gerät sind unbearbeitete Vorfälle vorhanden. Vorfälle	• Umschalter

unbearbeitete Vorfälle erkannt	können sowohl automatisch mithilfe von auf dem Client-Gerät installierten Verwaltungsprogrammen von Kaspersky als auch manuell durch den Administrator erstellt werden.	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 ermöglicht es, den Status eines Gerätes in einer Administrationsgruppe unter bestimmten Bedingungen automatisch zu ändern. Bei Erfüllung der festgelegten Bedingungen wird dem Client-Gerät einer der folgenden Statuswerte verliehen: *Kritisch* oder *Warnung*. Sind die festgelegten Bedingungen nicht erfüllt, so erhält das Client-Gerät den Status *OK*.

Verschiedenen Werten einer einzelnen Bedingung können verschiedene Statusvarianten entsprechen. Beispiele: Wenn die Bedingung **Die Datenbanken sind veraltet** den Wert **Über 3 Tage** besitzt, erhält das Client-Gerät standardmäßig den Status *Warnung*; für den Wert **Über 7 Tage** wird der Status *Kritisch* zugewiesen.

Wenn Sie Kaspersky Security Center Linux von der vorhergehenden Version upgraden, bleiben die Werte für die Zuweisung der Statusvarianten *Kritisch* oder *Warnung* für die Bedingung **Die Datenbanken sind veraltet** unverändert.

Wenn Kaspersky Security Center Linux 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. Öffnen Sie das Eigenschaftenfenster auf eine der folgenden Weisen:

   - Wählen Sie im Ordner **Richtlinien** im Kontextmenü der Richtlinie eines Administrationsservers **Eigenschaften** aus.

   - Wählen Sie im Kontextmenü einer Administrationsgruppe den Punkt **Eigenschaften** aus.

2. Wählen Sie im nächsten Eigenschaftenfenster im Bereich **Abschnitte** den Punkt **Gerätestatus** aus.

3. Aktivieren Sie im rechten Bereich im Abschnitt **Werte mit Status "Kritisch"** das Kontrollkästchen neben einer Bedingung in der Liste.

   Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

4. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.
   Sie können Werte für bestimmte Bedingungen festlegen, aber nicht für alle.

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

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Kritisch*.

Um die Änderungen des Gerätestatus auf Warnung zu aktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Eigenschaftenfenster auf eine der folgenden Weisen:

   - Wählen Sie im Ordner **Richtlinien** im Kontextmenü der Richtlinie des Administrationsservers den Punkt **Eigenschaften** aus.

   - Wählen Sie im Kontextmenü der Administrationsgruppe den Punkt **Eigenschaften** aus.

2. Wählen Sie im nächsten Eigenschaftenfenster im Bereich **Abschnitte** den Punkt **Gerätestatus** aus.

3. Aktivieren Sie im rechten Bereich im Abschnitt **Werte mit Status "Warnung"** das Kontrollkästchen neben einer Bedingung in der Liste.

   Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

4. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.
   Sie können Werte für bestimmte Bedingungen festlegen, aber nicht für alle.

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

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Warnung*.

Richtlinien und Richtlinienprofile

In Kaspersky Security Center 14 Web Console können Sie Richtlinien für Kaspersky-Apps erstellen. In diesem Abschnitt werden Richtlinien und Richtlinienprofile beschrieben, und Sie erhalten Anweisungen für deren Erstellung und Änderung.

Über Richtlinien und Richtlinienprofile

Eine *Richtlinie* besteht aus einer Reihe von 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 bietet eine einzelne Richtlinie für jedes Kaspersky-Programm in einer Administrationsgruppe. Eine Richtlinie hat eine der folgenden Statusvarianten:

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.
- 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 erfüllt ist.
- Richtlinienprofile enthalten Werte für Einstellungen, die von den Richtlinieneinstellungen abweichen.

- Durch das Aktivieren eines Richtlinienprofils werden die effektiven Einstellungen des verwalteten Gerätes geändert.
- Eine Richtlinie kann nicht mehr als 100 Richtlinienprofile enthalten.

Über das Schloss und gesperrte Einstellungen

Jede Richtlinieneinstellung verfügt über 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:

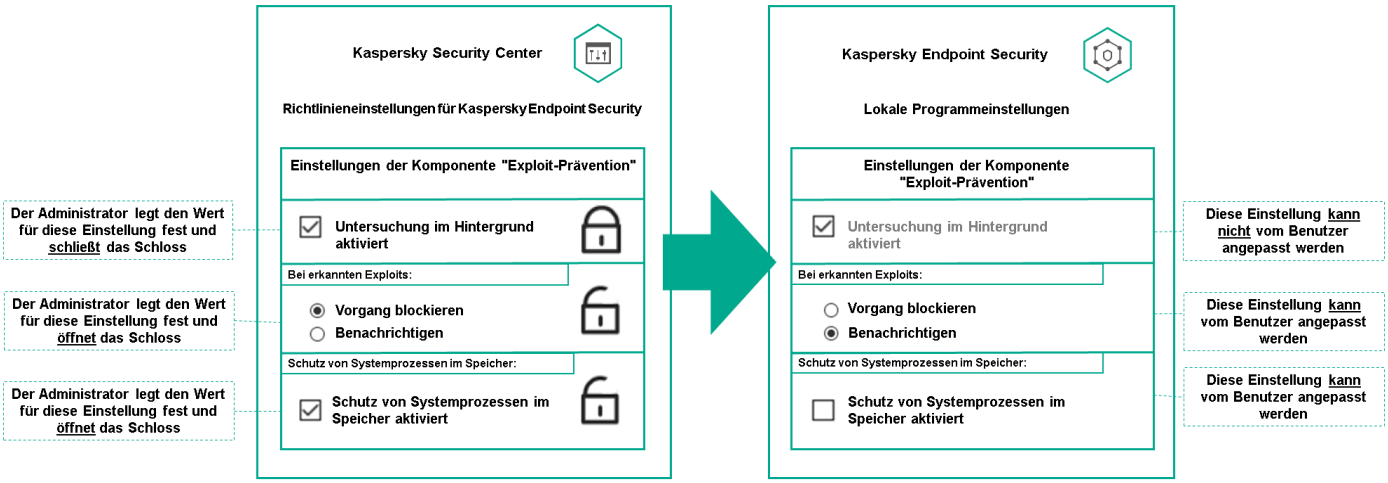
- Sperren von Einstellungen für eine Verwaltungsuntergruppenrichtlinie
- Sperren von Einstellungen eines Kaspersky-Programms auf einem verwalteten Gerät

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 lokales 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

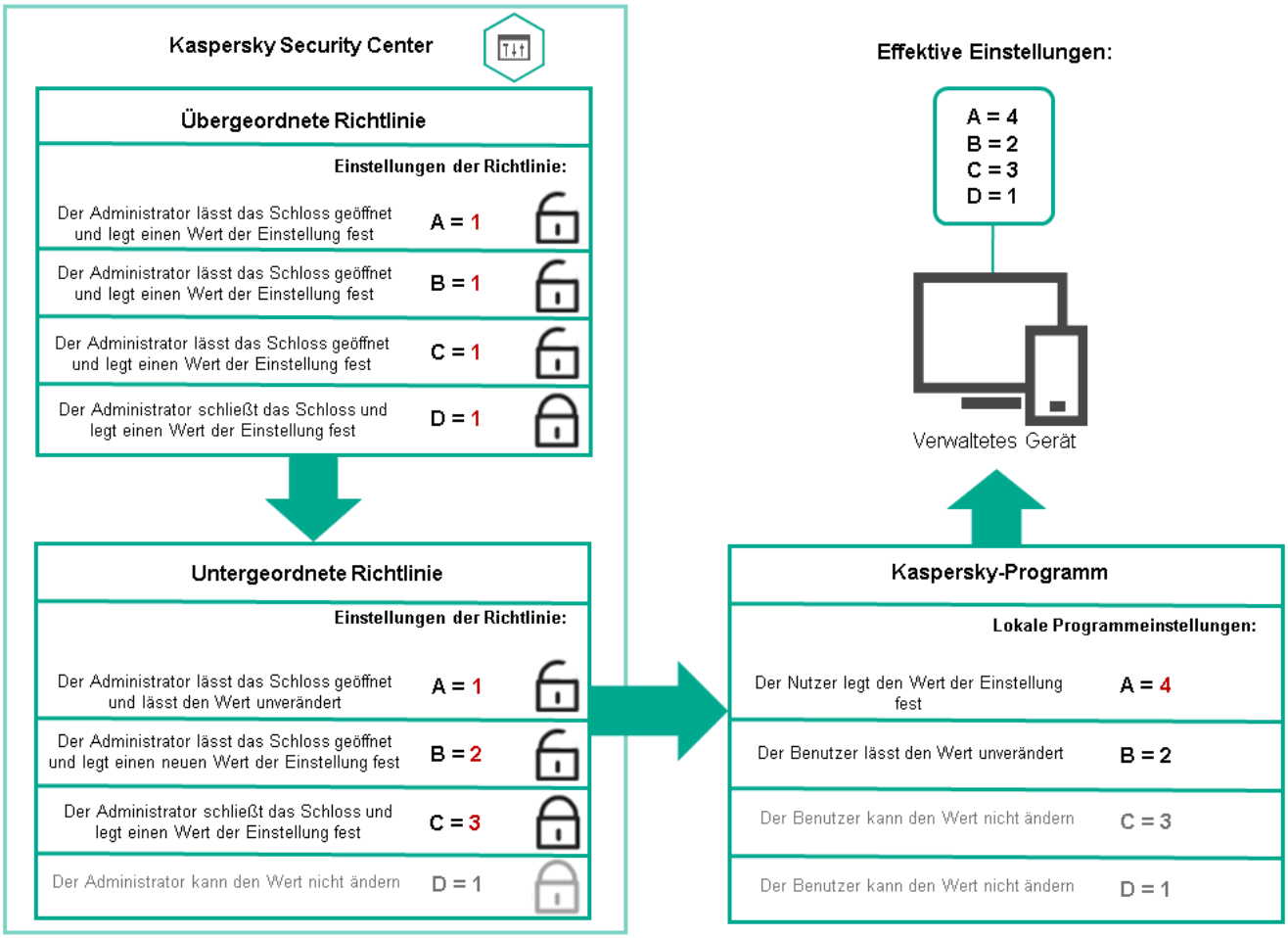
Wenn unterschiedliche Geräte unterschiedliche Einstellungen benötigen, können Sie Geräte in Administrationsgruppen organisieren.

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).

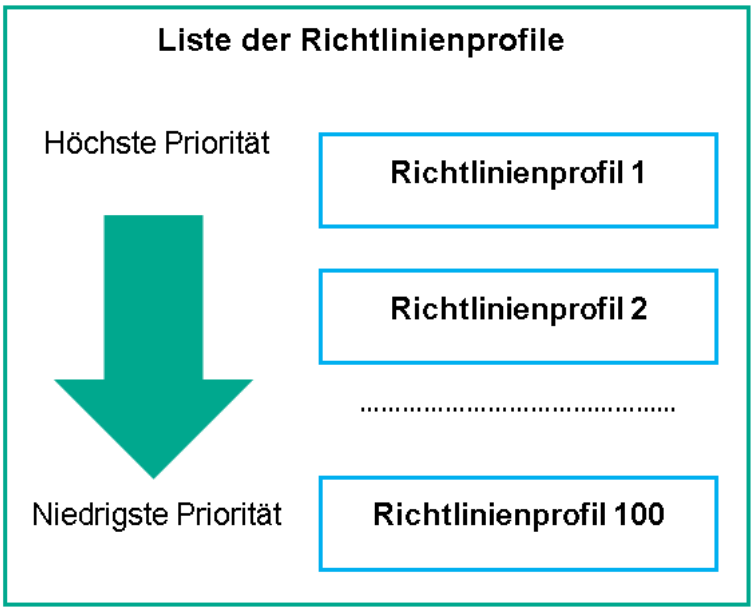


Hierarchie der Richtlinien

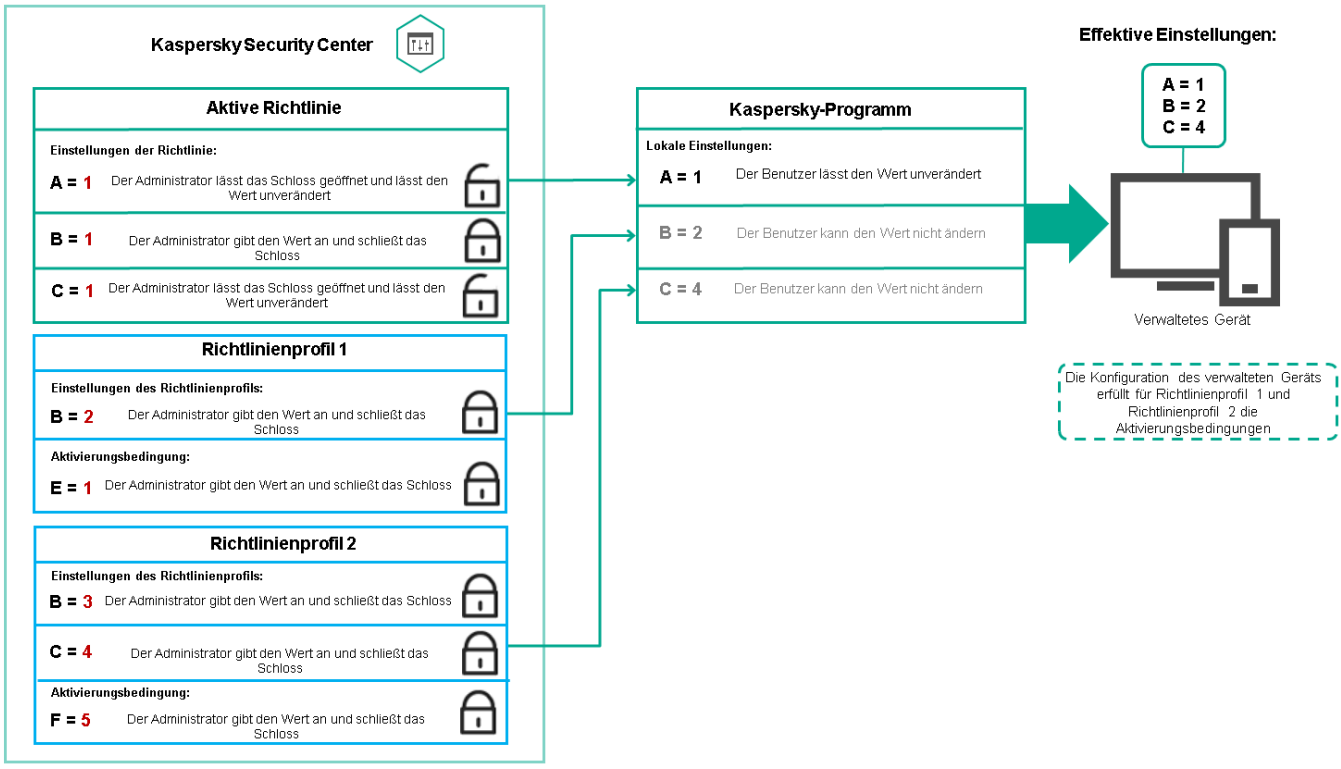
Richtlinienprofile in einer Hierarchie von Richtlinien

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).



- 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).



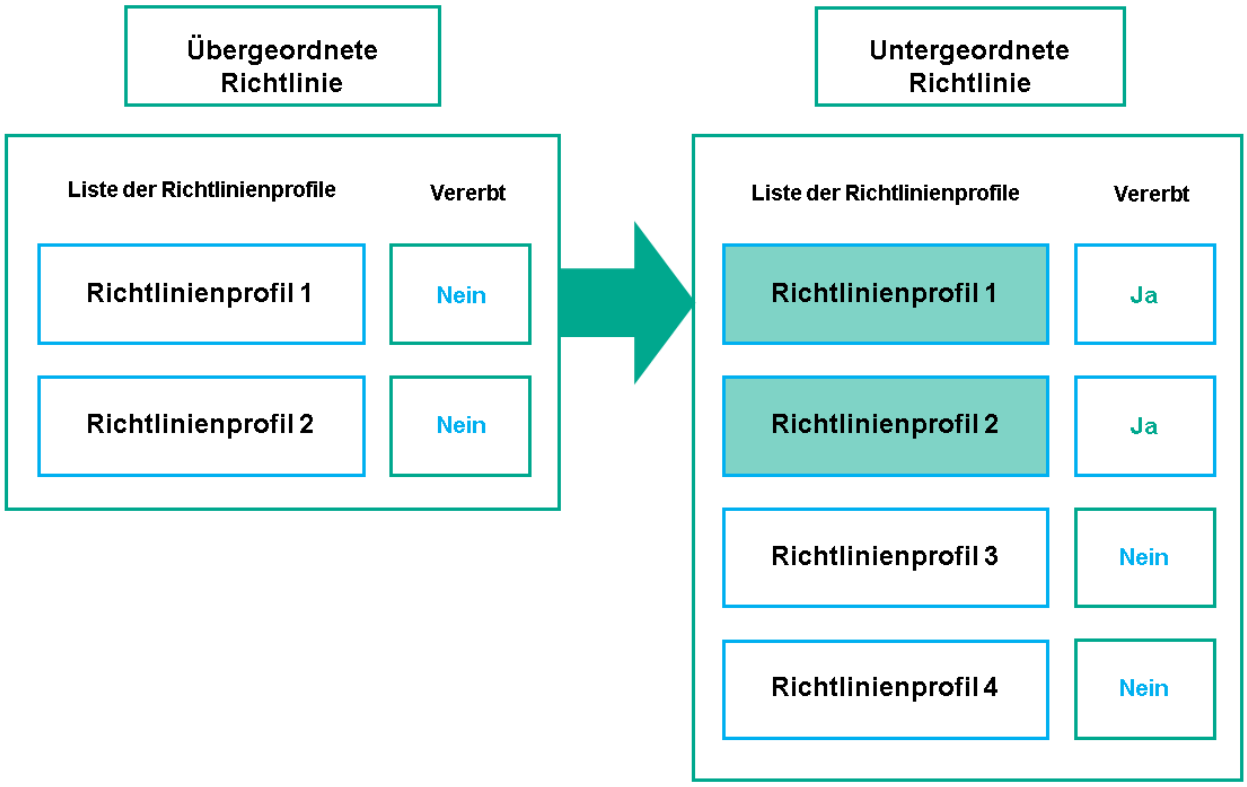
Die Konfiguration des verwalteten Geräts erfüllt die Aktivierungsbedingungen mehrerer Richtlinienprofile.

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).

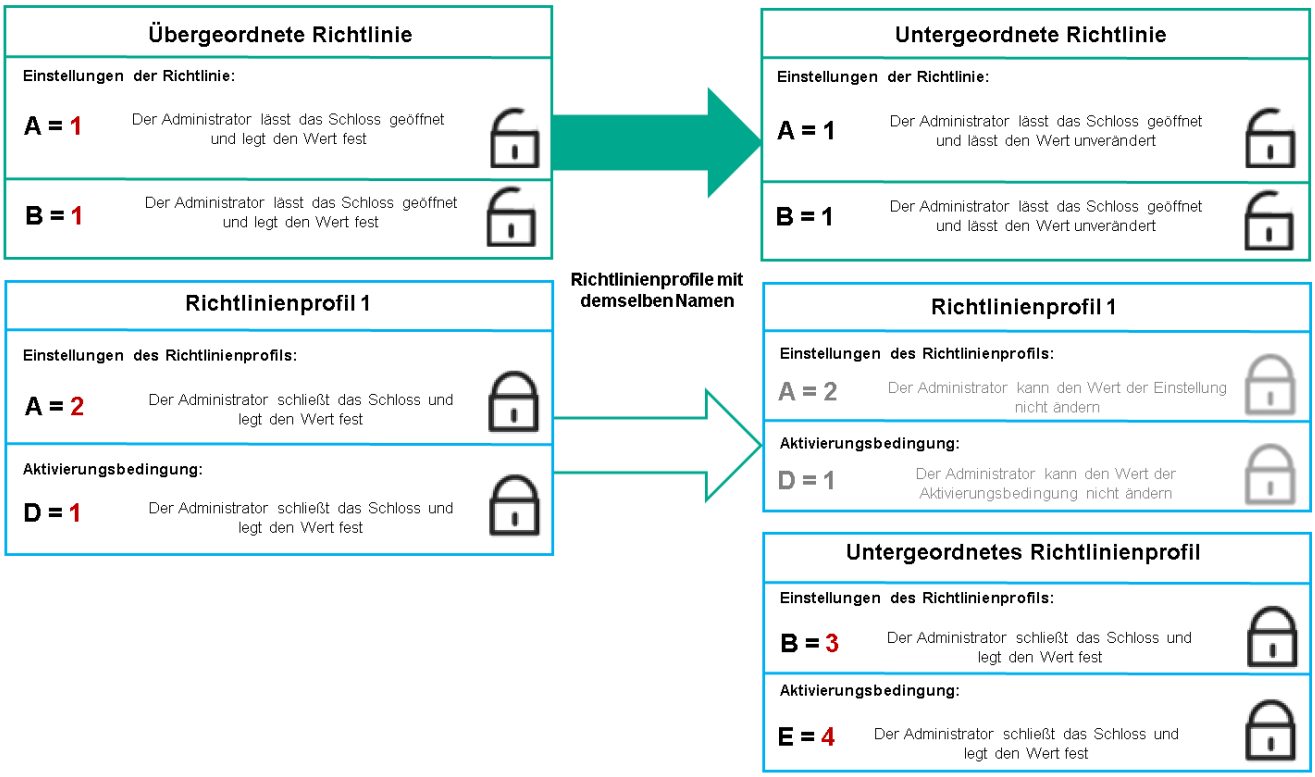


Vererbung von Richtlinienprofilen

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.

Um eine Richtlinie zu erstellen, gehen Sie wie folgt vor:

1. Gehen Sie 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. Wählen Sie die Registerkarte **Programmeinstellungen** aus.

   Sie können aber auch auf **Speichern** klicken und beenden. Die Richtlinie wird in der Liste der Richtlinien angezeigt, und Sie können ihre Einstellungen später anpassen.
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.

   Der Satz der Einstellungen ist davon abhängig, für welches Programm Sie eine Richtlinie erstellen. Weitere Informationen finden Sie hier:

   - Administrationsserver-Konfiguration
   - Richtlinieneinstellungen des Administrationsagenten
   - Hilfe zu Kaspersky Endpoint Security für Linux

   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.

Allgemeine Richtlinieneinstellungen

Allgemein

Auf der Registerkarte **Allgemein** können Sie den Richtlinienstatus ändern und die Vererbung der Richtlinieneinstellungen anpassen:

- Im Block **Richtlinienstatus** können Sie einen der Richtlinienmodi auswählen:
  - **Aktiv**

    Bei Auswahl dieser Option wird die Richtlinie aktiv.

    Diese Variante ist standardmäßig ausgewählt.

  - **Mobil**

    Bei Auswahl dieser Option wird die Richtlinie aktiv, sobald das Gerät vom Unternehmensnetzwerk getrennt wird.

  - **Inaktiv**

    Bei Auswahl dieser Option wird die Richtlinie inaktiv, aber im Ordner **Richtlinien** gespeichert. Bei Bedarf kann die Richtlinie aktiviert werden.

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

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

    Diese Option ist standardmäßig aktiviert.

  - **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 eingebetteten Administrationsgruppen, verbreitet.
- Im Block **Einstellungen erben** des Abschnitts **Allgemein** im Eigenschaftenfenster aller untergeordneten Richtlinien wird die Option **Einstellungen aus Richtlinie der höheren Ebene erben** automatisch aktiviert.

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

Diese Option ist standardmäßig deaktiviert.

Konfiguration von Ereignissen

Auf der Registerkarte **Konfiguration von Ereignissen** können Sie die Ereignisprotokollierung und die Benachrichtigung über Ereignisse konfigurieren. Die Ereignisse werden anhand der Ereigniskategorie auf folgende Registerkarten aufgeteilt:

- **Kritisch**

  Der Abschnitt **Kritisch** wird in den Eigenschaften der Richtlinie des Administrationsagenten nicht angezeigt.
- **Funktionsfehler**
- **Warnung**
- **Information**

Jeder Abschnitt enthält eine Liste mit Ereignistypen und der Standard-Speicherdauer des Ereignisses auf dem Administrationsserver (in Tagen). Mit einem Klick auf einen Ereignistyp können Sie die folgenden Einstellungen festlegen:

- **Ereignisregistrierung**

  Sie können angeben, wie viele Tage und an welchem Ort das Ereignis gespeichert werden soll:

  - **Mittels Syslog in ein SIEM-System exportieren**
  - **Im System-Ereignisprotokoll des Geräts speichern**
  - **Im System-Ereignisprotokoll des Administrationsservers speichern**
- **Ereignisbenachrichtigungen**

  Sie können bestimmen, ob Sie auf eine der folgenden Arten über das Ereignis benachrichtigt werden möchten:

  - **Per E-Mail benachrichtigen**
  - **Per SMS benachrichtigen**
  - **Durch den Start einer ausführbaren Datei oder eines Skriptes benachrichtigen**
  - **Per SNMP benachrichtigen**

Standardmäßig werden die Benachrichtigungseinstellungen verwendet, die auf der Registerkarte "Eigenschaften des Administrationsservers" angegeben sind (z. B. Empfängeradresse). Wenn Sie möchten, können Sie diese Einstellungen auf den Registerkarten **E-Mail**, **SMS** und **Start einer ausführbaren Datei** ändern.

Revisionsverlauf

Auf der Registerkarte **Revisionsverlauf** können Sie eine Liste mit Revisionen der Richtlinie anzeigen und bei Bedarf ein Rollback der Änderungen an der Richtlinie vornehmen.

Richtlinie ändern

Um eine Richtlinie zu ändern, gehen Sie wie folgt vor:

1. Gehen Sie 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
   - Hilfe zu Kaspersky Endpoint Security für Linux

   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.

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 **Uhrzeit der Verschlüsselung**, 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 **Uhrzeit der Verschlüsselung**, 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).

Erzwungene Synchronisierung

Obwohl Kaspersky Security Center Linux den Status, die Einstellungen, die Aufgaben und die Richtlinien für die verwalteten Geräte automatisch synchronisiert, kann es in bestimmten Situationen vorkommen, dass der Administrator genau wissen muss, 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. Gehen Sie 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:

   - Gehen Sie 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 kann der Administrator auch prüfen, ob die geänderte Richtlinie an ein bestimmtes verwaltetes Gerät übermittelt wurde. Eine Richtlinie kann während einer regulären oder einer erzwungenen Synchronisierung übermittelt werden.

Um den Zeitpunkt (Datum und Uhrzeit) anzuzeigen, zu dem eine Programmrichtlinie an ein verwaltetes Gerät übermittelt wurde:

1. Gehen Sie 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.

Anzeigen des Statusdiagramms für die Richtlinienverteilung

In Kaspersky Security Center können Sie den Übernahmestatus einer Richtlinie für jedes Gerät in einem Statusdiagramm zur Richtlinienverteilung anzeigen.

Um das Statusdiagramm für die Richtlinienverteilung für jedes Gerät anzuzeigen, gehen Sie wie folgt vor:

1. Gehen Sie 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. Wählen Sie im sich öffnenden Menü den Link **Verteilung**.

Das Fenster **<Name der Richtlinie> Ergebnisse der Verteilung** wird geöffnet.

4. Im geöffneten Fenster **<Name der Richtlinie> Ergebnisse der Verteilung** wird eine **Statusbeschreibung** der Richtlinie angezeigt.

Sie können die Anzahl der angezeigten Ergebnisse in der Liste der Richtlinienverteilung ändern. Die maximale Anzahl an Geräten ist 100.000.

Um die Anzahl der in der Liste mit den Ergebnissen der Richtlinienverteilung angezeigten Geräte zu ändern, gehen Sie wie folgt vor:

1. Gehen Sie zum Abschnitt **Einstellungen der Benutzeroberfläche** in der Symbolleiste.
2. Geben Sie für **Obergrenze der in den Ergebnissen der Richtlinienverteilung angezeigten Geräte** die Anzahl an Geräten ein (bis zu 100.000).

   Die standardmäßige Anzahl beträgt 5000.
3. Klicken Sie auf die Schaltfläche **Speichern**.

   Ihre Einstellungen werden gespeichert und übernommen.

Richtlinien löschen

Eine nicht mehr benötigte Richtlinie kann gelöscht werden. Sie können nur Richtlinien löschen, die in der angegebenen Administrationsgruppe nicht geerbt sind. Eine geerbte Richtlinie kann nur in der Gruppe der höheren Ebene gelöscht werden, für die sie erstellt wurde.

Um eine Richtlinie zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **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 **Uhrzeit der Verschlüsselung**, 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 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 die Tabelle leer 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 für die gewünschte Richtlinie in die Liste der Profile.

   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 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.
       - **Maximale Kapazität des Dienstes wurde überschritten** – 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).

  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 Linux anzupassen und zu aktivieren. In der Dropdown-Liste unter diesem Kontrollkästchen können die Kriterien für die Aktivierung des Profils ausgewählt werden:

  - Der Gerätebesitzer gehört zur angegebenen Sicherheitsgruppe ("="-Symbol).
  - Der Gerätebesitzer gehört nicht zur angegebenen Sicherheitsgruppe ("#"-Symbol).

    Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt. Sie können eine Sicherheitsgruppe für Kaspersky Security Center Linux 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:

  - Liste der Tags

    Geben Sie in der Liste der Tags Aktivierungsregeln für Geräte im Richtlinienprofil an, indem Sie die Kontrollkästchen der entsprechenden Tags aktivieren.

    Sie können neue Tags zur Liste hinzufügen, indem Sie diese im Feld über der Liste eingeben und auf die Schaltfläche **Hinzufügen** klicken.

    Das Richtlinienprofil erstreckt sich auf Geräte, in deren Beschreibung alle ausgewählten Tags vorkommen. Sind Kontrollkästchen deaktiviert, wird das Kriterium nicht angewandt. Standardmäßig sind die Kontrollkästchen deaktiviert.

  - Auf Geräte ohne angegebene Tags anwenden

    Aktivieren Sie die Option, wenn die Auswahl der Tags invertiert werden muss.

    Wenn diese Option aktiviert ist, werden Geräte, in deren Beschreibung keines der gewählten Tags vorkommt, in das Richtlinienprofil aufgenommen. Wenn diese Option deaktiviert ist, wird das Kriterium nicht angewendet.

    Diese Option ist standardmäßig deaktiviert.

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.

Benutzer und Benutzerrollen

In diesem Abschnitt werden Benutzer und Benutzerrollen beschrieben und Anweisungen zum Erstellen und Ändern dieser Regeln, zum Zuweisen von Rollen und Gruppen zu Benutzern sowie zum Zuordnen von Richtlinienprofilen zu Rollen zur Verfügung gestellt.

Über Benutzerrollen

Eine *Benutzerrolle* (auch als *Rolle* bezeichnet) ist ein Objekt, das einen Satz von Rechten und Berechtigungen enthält. Eine Rolle kann mit Einstellungen von Anwendungen von Kaspersky verbunden sein, die auf einem Benutzergerät installiert sind. Sie können eine Rolle einem Satz von Bedingungen oder einem Satz von Sicherheitsgruppen auf jeder Ebene der Hierarchie von Administrationsgruppen zuweisen.

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 Linux bietet Unterstützungen für eine rollenbasierte Zugriffskontrolle auf die Funktionen von Kaspersky Security Center Linux und von verwalteten Kaspersky-Programmen an.

Sie können die Zugriffsrechte auf Programmfunktionen für Benutzer von Kaspersky Security Center Linux 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 unten stehende Tabelle gibt die Funktionen von Kaspersky Security Center Linux 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**, **Ändern** 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**	**Ändern**	• Hinzufügen eines Geräts zu einer Administrationsgruppe: **Ändern** • Löschen eines Geräts aus einer Administrationsgruppe: **Ändern** • Hinzufügen einer Administrationsgruppe zu einer anderen Administrationsgruppe: **Ändern** • Löschen einer Administrationsgruppe aus einer anderen Administrationsgruppe: **Ändern**	Nichts
Allgemeine Funktionen: **Zugriff auf Objekte, unabhängig von ihren ACLs**	**Lesen**	Lesenden Zugriff auf alle Objekte bekommen: **Lesen**	Nichts
Allgemeine Funktionen: **Grundlegende Funktionen**	• **Lesen** • **Ändern**	• Regeln für das Verschieben von Geräten (erstellen, ändern, löschen) für den virtuellen	• "Download von U in die Datenverw des Administrations

	• **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	Server: **Ändern**, **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: **Ändern** • Liste der Zugriffskontrolle von Gruppen anzeigen: **Lesen** • Ereignisprotokoll "Kaspersky" anzeigen: **Lesen**	• "Berichte sende • "Installationspak verteilen" • "Remote-Installa eines Programm sekundären Administrations

Allgemeine Funktionen: **Gelöschte Objekte**	• **Lesen** • **Ändern**	• Gelöschte Objekte im Papierkorb anzeigen: **Lesen** • Objekte aus dem Papierkorb löschen: **Ändern**	Nichts
Allgemeine Funktionen: **Verarbeitung von Ereignissen**	• **Ereignisse löschen** • **Einstellungen der Ereignisbenachrichtigung bearbeiten** • **Einstellungen der Ereignisprotokollierung bearbeiten** • **Ändern**	• Einstellungen der Ereignisregistrierung ändern: **Einstellungen der Ereignisprotokollierung bearbeiten** • Einstellungen der Ereignisbenachrichtigung ändern: **Einstellungen der Ereignisbenachrichtigung bearbeiten** • Ereignisse löschen: **Ereignisse löschen**	Nichts
Allgemeine Funktionen: **Vorgänge auf dem Administrationsserver**	• **Lesen** • **Ändern** • **Ausführen** • **Objekt-ACLs ändern** • **Vorgänge auf Geräteauswahlen ausführen**	• Ports des Administrationsservers für die Verbindung zum Administrationsagenten angeben: **Ändern** • Ports des auf dem Administrationsserver gestarteten Aktivierungsproxy angeben: **Ändern** • Ports des auf dem Administrationsserver gestarteten Aktivierungsproxy für mobile Geräte angeben: **Ändern** • Ports des Webservers für die Verteilung von autonomen Paketen angeben: **Ändern** • Ports des Webservers für die Verteilung von MDM-Profilen angeben: **Ändern** • SSL-Ports des Administrationsservers für	• "Backup der Dat Administrationss anlegen" • "Pflege von Datenbanken"

		die Verbindung mittels Web Console angeben: **Ändern** • Ports des Administrationsservers für die Verbindung mit mobilen Geräten angeben: **Ändern** • Maximale Anzahl von Ereignissen, die in der Datenbank des Administrationsservers gespeichert sind, angeben: **Ändern** • Maximale Anzahl von Ereignissen, die der Administrationsserver versenden kann, angeben: **Ändern** • Zeitspanne, in welcher Ereignisse durch den Administrationsserver versendet werden können, angeben: **Ändern**	
Allgemeine Funktionen: **Verteilung von Programmen von Kaspersky**	• **Patches von Kaspersky verwalten** • **Lesen** • **Ändern** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	Die Installation von Patches akzeptieren oder ablehnen: **Patches von Kaspersky verwalten**	Nichts
Allgemeine Funktionen: **Schlüsselverwaltung**	• **Schlüsseldatei exportieren** • **Ändern**	• Schlüsseldatei exportieren: **Schlüsseldatei exportieren**	Nichts

		• Einstellungen des Lizenzschlüssels des Administrationsservers ändern: **Ändern**	
Allgemeine Funktionen: **Erzwungene Berichtsverwaltung**	• **Lesen** • **Ändern**	• 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** • **Ändern** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	• Liste mit virtuellen Administrationsservern abrufen: **Lesen** • Informationen über den virtuellen Administrationsserver erhalten: **Lesen** • Virtuellen Administrationsserver erstellen, aktualisieren oder löschen: **Virtuelle**	Nichts

		Administrationsserver verwalten • Virtuellen Administrationsserver in andere Gruppe verschieben: **Virtuelle Administrationsserver verwalten** • Rechte des virtuellen Administrationsservers angeben: **Virtuelle Administrationsserver verwalten**	

Vorkonfigurierte Benutzerrollen

Benutzer von Kaspersky Security Center Linux mit zugewiesenen Benutzerrollen bekommen Zugriffsrechte auf Programmfunktionen gewährt.

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 Linux verfügbaren vordefinierten Benutzerrollen können bestimmten Positionen zugeordnet werden, z. B. **Auditor**, **Sicherheitsbeauftragter** oder **Supervisor**. 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 **Ändern** 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.

Die Funktionen der Funktionsbereiche **Mobile Geräte verwalten: Allgemein** und **Systemverwaltung** sind in Kaspersky Security Center Linux nicht verfügbar. Ein Benutzer mit den Rollen **Administrator von 'Schwachstellen- und Patch-Management'/Operator** und **Administrator von 'Mobile Geräte verwalten'/Operator** hat nur Zugriff auf die Berechtigungen des Funktionsbereichs **Allgemeine Funktionen**: **Basic**.

Zugriffsberechtigungen von vorkonfigurierten Benutzerrollen

Rolle	Beschreibung

Administrator des Administrationsserver	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen in **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Verarbeitung von Ereignissen** • **Hierarchie des Administrationsservers** • **Virtuelle Administrationsserver**
Operator des Administrationsserver	Gewährt die Berechtigungen **Lesen** und **Ausführen** in allen folgenden Funktionsbereichen innerhalb von **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Virtuelle Administrationsserver**
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 in **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Verteilung der Software von Kaspersky** • **Verwaltung von Lizenzschlüsseln** Gewährt die Berechtigungen **Lesen** und **Ausführen** in dem Funktionsbereich **Allgemeine Funktionen: Virtuelle Administrationsserver**.
Installationsoperator	Gewährt die Berechtigungen **Lesen** und **Ausführen** in allen folgenden Funktionsbereichen innerhalb von **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Kaspersky Softwareverteilung** (gewährt auch die Berechtigung **Verwaltung von Kaspersky Lab-Patches** in diesem Bereich) • **Virtuelle Administrationsserver**
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
Operator von Kaspersky	Gewährt die Berechtigungen **Lesen** und **Ausführen** in allen folgenden

Endpoint Security	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**
Hauptoperator	Gewährt die Berechtigungen **Lesen** und **Ausführen** (falls anwendbar) in allen folgenden Funktionsbereichen: • **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Gelöschte Objekte** • **Vorgänge auf dem Administrationsserver** • **Kaspersky Lab Softwareverteilung** • **Virtuelle Administrationsserver** • Alle Funktionen aus dem Bereich von Kaspersky Endpoint Security
Administrator der Funktion "Mobile Geräte verwalten"	Erlaubt alle Operationen im Funktionsbereich **Allgemeine Funktionen: Basisfunktionen**.
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**, **Ändern**, **Ausführen**, **Dateien von Geräten auf dem Administrator-Arbeitsplatz speichern** und **Ausführen von Vorgängen für die Geräteauswahlen** im Funktionsbereich **Systemverwaltung: Verbindungen**. Sie können diese Rolle einem Beauftragten zuweisen, der für die IT-Sicherheit in Ihrer Organisation zuständig ist.
Benutzer des Self Service Portals	Erlaubt alle Vorgänge im Funktionsbereich **Mobile Geräte verwalten: Self Service Portal**. Diese Funktionen wird nur von Kaspersky Security Center 11 oder höher unterstützt.
Supervisor	Gewährt die Berechtigung **Lesen** in den Funktionsbereichen **Allgemeine Funktionen**: **Zugriff auf Objekte, unabhängig von ihren ACLs** und **Allgemeine Funktionen**: **Erzwungene Berichtsverwaltung**. Sie können diese Rolle einem Security Officer und anderen Verantwortlichen zuweisen, die für die IT-Sicherheit in Ihrer Organisation zuständig sind.

Hinzufügen eines Benutzerkontos eines internen Benutzers

Um ein neues internes Benutzerkonto zu Kaspersky Security Center Linux hinzuzufügen:

1. Wechseln Sie im Hauptmenü zu **BENUTZER UND ROLLEN** → **BENUTZER**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Geben Sie im folgenden Fenster **Neue Entität** die Einstellungen des neuen Benutzerkontos an:
   - Behalten Sie die Standardoption **Benutzer** bei.
   - **Das APNs-Zertifikat läuft bald ab**.
   - **Kennwort** für die Verbindung des Benutzers mit Kaspersky Security Center Linux.
     Das Kennwort muss den folgenden Regeln entsprechen:
     - Das Kennwort muss zwischen 8 und 16 Zeichen lang sein
     - Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Gruppen enthalten:
       - Großbuchstaben (A–Z)
       - Kleinbuchstaben (a–z)
       - Zahlen (0–9)
       - Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - In einem Kennwort sind unzulässig: Leerzeichen, Unicode-Zeichen oder die Kombination von "." und "@", falls "." vor "@" steht.

     Um die von Ihnen eingegebenen Zeichen anzuzeigen, klicken Sie die Schaltfläche **Anzeigen** und halten Sie diese gedrückt.

     Die Anzahl der Eingabeversuche für das Kennwort ist beschränkt. Standardmäßig beträgt die maximale Anzahl der Eingabeversuche für das Kennwort 10. Sie können die zulässige Anzahl der Versuche zur Eingabe eines Kennworts ändern (siehe Beschreibung unter Anzahl der erlaubten Kennworteingabeversuche).

     Wenn der Benutzer das Kennwort innerhalb der angegebenen Anzahl von Versuchen nicht korrekt eingegeben hat, wird das Benutzerkonto für eine Stunde gesperrt. Sie können das Benutzerkonto nur durch die Änderung des Kennworts entsperren.
   - **Vollständiger Name**
   - **Beschreibung**
   - **E-Mail-Adresse**

- **Telefon**

4. Klicken Sie auf die Schaltfläche **Uhrzeit der Verschlüsselung**, um die Änderungen zu speichern.

Das neue Benutzerkonto wird in der Liste der Benutzer und Benutzergruppen angezeigt.

Erstellen einer Benutzergruppe

So erstellen Sie eine Benutzergruppe:

1. Wechseln Sie im Hauptmenü zu **BENUTZER UND ROLLEN** → **BENUTZER**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Wählen Sie im folgenden Fenster **Neue Entität** den Punkt **Gruppe** aus.
4. Geben Sie die folgenden Einstellungen für die neue Benutzergruppe an:
   - **Gruppenname**
   - **Beschreibung**
5. Klicken Sie auf die Schaltfläche **Uhrzeit der Verschlüsselung**, um die Änderungen zu speichern.

Die neue Benutzergruppe wird in der Liste der Benutzer und Benutzergruppen angezeigt.

Bearbeiten eines Benutzerkontos eines internen Benutzers

Um ein internes Benutzerkonto in Kaspersky Security Center Linux zu bearbeiten:

1. Wechseln Sie im Hauptmenü zu **BENUTZER UND ROLLEN** → **BENUTZER**.
2. Klicken Sie auf den Namen des Benutzerkontos, das Sie bearbeiten möchten.
3. Ändern Sie im folgenden Fenster für Benutzereinstellungen auf der Registerkarte **Allgemein** die Einstellungen für das Benutzerkonto:
   - **Beschreibung**
   - **Vollständiger Name**
   - **E-Mail-Adresse**
   - **Hauptrufnummer**
   - **Kennwort** für die Verbindung des Benutzers mit Kaspersky Security Center Linux.
     Das Kennwort muss den folgenden Regeln entsprechen:
     - Das Kennwort muss zwischen 8 und 16 Zeichen lang sein

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

Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen**.

> Die Anzahl der Eingabeversuche für das Kennwort ist beschränkt. Standardmäßig beträgt die maximale Anzahl der Eingabeversuche für das Kennwort 10. Sie können die zulässige Anzahl an Versuchen ändern, es wird jedoch aus Sicherheitsgründen nicht empfohlen, diese Zahl zu verringern. Wenn der Benutzer das Kennwort innerhalb der angegebenen Anzahl von Versuchen nicht korrekt eingegeben hat, wird das Benutzerkonto für eine Stunde gesperrt. Sie können das Benutzerkonto nur durch die Änderung des Kennworts entsperren.

- Schalten Sie ggf. die Umschalttaste auf **Deaktiviert**, um zu verhindern, dass der Benutzer eine Verbindung zur Anwendung herstellt. Sie können ein Konto beispielsweise deaktivieren, nachdem ein Mitarbeiter das Unternehmen verlassen hat.

4. Auf der Registerkarte **Sicherheit für die Authentifizierung** können Sie die Sicherheitseinstellungen für dieses Benutzerkonto festlegen.
5. Auf der Registerkarte **Gruppen** können Sie einen Benutzer zu Sicherheitsgruppen hinzufügen.
6. Auf der Registerkarte **Geräte** können Sie einem Benutzer Geräte zuweisen.
7. Auf der Registerkarte **Rollen** können Sie einem Benutzer Rollen zuordnen.
8. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Das aktualisierte Benutzerkonto wird in der Liste der Benutzer und Sicherheitsgruppen angezeigt.

Bearbeiten einer Benutzergruppe

> Sie können nur interne Gruppen löschen.

So bearbeiten Sie eine Benutzergruppe:

1. Wechseln Sie im Hauptmenü zu **BENUTZER UND ROLLEN** → **BENUTZER**.
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:

- **Das APNs-Zertifikat läuft bald ab**
- **Beschreibung**

4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die aktualisierte Gruppe wird in der Liste der Benutzer und Benutzergruppen angezeigt.

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**.
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.

Festlegen eines Benutzers als Gerätebesitzer

Informationen zum Festlegen eines Benutzers als Besitzer eines mobilen Geräts finden Sie in der Hilfe von Kaspersky Security für mobile Endgeräte.

So weisen Sie einen Benutzer als Gerätebesitzer zu:

1. Wechseln Sie im Hauptmenü zu **BENUTZER UND ROLLEN** → **BENUTZER**.
2. Klicken Sie auf den Namen des Benutzerkontos, das Sie als Gerätebesitzer zuweisen möchten.
3. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Geräte**.
4. Klicken Sie auf die Schaltfläche **Hinzufügen**.
5. Wählen Sie in der Geräteliste die Richtlinie aus, die Sie dem Benutzer zuweisen möchten.
6. Klicken Sie auf die Schaltfläche **Uhrzeit der Verschlüsselung**.

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**.

Löschen eines Benutzers oder einer Sicherheitsgruppe

Sie können nur interne Benutzer oder interne Sicherheitsgruppen löschen.

So löschen Sie einen Benutzer oder eine Sicherheitsgruppe:

1. Wechseln Sie im Hauptmenü zu **BENUTZER UND ROLLEN → BENUTZER**.
2. Aktivieren Sie das Kontrollkästchen neben dem Benutzer oder neben der Sicherheitsgruppe, den oder die Sie entfernen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie im folgenden Fenster auf **Uhrzeit der Verschlüsselung**.

Der Benutzer oder die Sicherheitsgruppe ist gelöscht.

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 **Uhrzeit der Verschlüsselung**, 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.

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, Sicherheitsgruppen und Administrationsgruppen zum Bereich einer Benutzerrolle hinzuzufügen, können Sie eine der folgenden Methoden anwenden:

Methode 1:

1. Wechseln Sie im Hauptmenü zu **BENUTZER UND ROLLEN** → **BENUTZER**.
2. Aktivieren Sie die Kontrollkästchen neben den Benutzern und Sicherheitsgruppen, die Sie dem Benutzerrollenbereich hinzufügen möchten.
3. Klicken Sie auf die Schaltfläche **Rolle zuordnen**.

   Der Rollenzuweisungs-Assistent 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** die Administrationsgruppe aus, die Sie dem Gültigkeitsbereich der Benutzerrolle hinzufügen möchten.
6. Klicken Sie auf die Schaltfläche **Rolle zuordnen**, um den Assistenten zu schließen.

Die ausgewählten Benutzer oder Sicherheitsgruppen 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 Rollenzuweisungs-Assistent wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.
5. Wählen Sie auf der Seite **Bereich definieren** die Administrationsgruppe aus, die Sie dem Gültigkeitsbereich der Benutzerrolle hinzufügen möchten.
6. Wählen Sie auf der Seite **Benutzer auswählen** des Assistenten die Benutzer und Sicherheitsgruppen aus, die Sie dem Gültigkeitsbereich der Benutzerrolle hinzufügen möchten.
7. Klicken Sie auf die Schaltfläche **Rolle zuordnen**, um den Assistenten zu schließen.
8. Klicken Sie auf die Schaltfläche **Schließen** ( ), um das Fenster der Rolleneigenschaften zu schließen.

Die ausgewählten Benutzer oder Sicherheitsgruppen 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 **Uhrzeit der Verschlüsselung**.

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.

Arbeit mit den Revisionen der Objekte

Der Abschnitt enthält Informationen über die Arbeit mit den Revisionen des Objekts. Kaspersky Security Center Linux erlaubt eine Nachverfolgung der Änderungen von Objekten. Jedes Mal, wenn Sie die Änderungen des Objektes speichern, wird eine *Revision* erstellt. Jede Revision hat eine Nummer.

Folgende Objekte des Programms unterstützen die Arbeit mit Revisionen:

- Administrationsserver
- Richtlinien
- Aufgaben
- Administrationsgruppen
- Benutzerkonten
- Installationspakete

Sie können mit den Revisionen von Objekten folgende Aktionen ausführen:

- Ausgewählte Revisionen mit der laufenden Revision vergleichen
- Ausgewählte Revisionen vergleichen
- Objekt mit der ausgewählten Revision eines anderen gleichartigen Objekts vergleichen
- Ausgewählte Revision anzeigen
- Rollback der Änderungen des Objektes auf die ausgewählte Revision durchführen
- Revisionen in eine Datei im txt-Format speichern

Im Eigenschaftenfenster der Objekte, die Revisionen unterstützen, wird im Abschnitt **Revisionsverlauf** eine Liste der Objektrevisionen mit den folgenden Informationen angezeigt:

- Nummer der Revision des Objekts
- Datum und Uhrzeit der Objektänderung
- Name des Benutzers, der das Objekt geändert hat
- Ausgeführte Aktion mit dem Objekt
- Beschreibung der Revision der Änderungen der Objekteinstellungen

  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**. Geben Sie im Fenster **Beschreibung der Revision des Objekts** einen Text zur Beschreibung der Revision ein.

Über Revisionen von Objekten

Sie können mit den Revisionen von Objekten folgende Aktionen ausführen:

- Ausgewählte Revisionen mit der laufenden Revision vergleichen
- Ausgewählte Revisionen vergleichen
- Objekt mit der ausgewählten Revision eines anderen gleichartigen Objekts vergleichen

- Ausgewählte Revision anzeigen
- Rollback der Änderungen des Objektes auf die ausgewählte Revision durchführen
- Revisionen in eine Datei im txt-Format speichern

Im Eigenschaftenfenster der Objekte, die Revisionen unterstützen, wird im Abschnitt **Revisionsverlauf** eine Liste der Objektrevisionen mit den folgenden Informationen angezeigt:

- Nummer der Revision des Objekts
- Datum und Uhrzeit der Objektänderung
- Name des Benutzers, der das Objekt geändert hat
- Ausgeführte Aktion mit dem Objekt
- Beschreibung der Revision der Änderungen der Objekteinstellungen

Rollback eines Objekts zu einer früheren Version

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. Wählen Sie im Eigenschaftenfenster des Objekts die Registerkarte **Revisionsverlauf** aus.
2. Wählen Sie in der Liste mit den Revisionen des Objekts die Revision aus, auf deren Stand die Änderungen zurückgesetzt werden sollen.
3. Klicken Sie auf die Schaltfläche **Rollback**.
4. Klicken Sie auf **Uhrzeit der Verschlüsselung**, um den Vorgang zu bestätigen.

   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.

Der Rollback-Vorgang ist nur für Richtlinien- und Aufgabenobjekte verfügbar.

Löschen von Objekten

Dieser Abschnitt bietet Informationen über das Löschen von Objekten und Anzeigen von Informationen über Objekte, nachdem sie gelöscht wurden.

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.

Verwendung des klscflag-Dienstprogramms, um Port 13291 zu öffnen

Auf dem Administrationsserver wird Port 13291 zum Empfangen der Verbindungen von Verwaltungskonsolen verwendet. Auf Nicht-Windows-Computern ist dieser Port standardmäßig nicht geöffnet. Wenn Sie die MMC-basierte Verwaltungskonsole oder das klakaut-Tool verwenden möchten, können Sie diesen Port über das klscflag-Tool öffnen. Dieses Tool ändert den Wert des Parameters KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Um den Port 13291 zu öffnen:

1. Führen Sie den folgenden Befehl in der Befehlszeile aus:
   ```
   $ klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
   ```
2. Starten Sie den Dienst des Kaspersky Security Center Administrationsservers neu, indem Sie den folgenden Befehl ausführen:
   ```
   $ sudo systemctl restart kladminserver_srv
   ```

   Der Port 13291 ist geöffnet.

Um zu überprüfen, ob Port 13291 erfolgreich geöffnet wurde:

Führen Sie den folgenden Befehl in der Befehlszeile aus:

```
$ klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

Dieser Befehl gibt das folgende Ergebnis zurück:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)true
```

Der Wert `true` bedeutet, dass der Port geöffnet ist. Andernfalls wird der Wert `false` angezeigt.

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 des Kaspersky Security Centers 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 "Netzwerkschutz konfigurieren" abgeschlossen haben, müssen Sie die Verlässlichkeit des Schutzsystems aufrecht erhalten, um sicherzustellen, dass die Administrationsserver und die verwalteten Geräte dauerhaft gegen verschiedene Bedrohungen wie Viren, Netzwerkangriffe und Phishing-Attacken geschützt sind.

Der Netzwerkschutz bleibt auf dem neuesten Stand, wenn folgende Komponenten regelmäßig aktualisiert werden:

- Kaspersky-Datenbanken und Programm-Module
- Installierte Programme von Kaspersky, einschließlich der Komponenten des Kaspersky Security Centers und der Sicherheitsanwendungen

Wenn Sie dieses Szenario abschließen, können Sie sicher sein, dass:

- Ihr Netzwerk durch die aktuellsten Programme von Kaspersky, einschließlich der Komponenten von Kaspersky Security Center Linux und der Sicherheitsanwendungen, geschützt ist.
- die Antiviren-Datenbanken und andere, für die Sicherheit des Netzwerks kritische Kaspersky-Datenbanken, immer auf dem neuesten Stand sind.

Erforderliche Maßnahmen

Die verwalteten Geräte benötigen eine Verbindung zum Administrationsserver. Wenn keine Verbindung besteht, können Sie das Update der Kaspersky-Datenbanken und der Programm-Module auch manuell oder direkt über die Kaspersky-Update-Server durchführen.

Der Administrationsserver muss eine Verbindung zum Internet haben.

Bevor Sie beginnen, stellen Sie sicher, dass Sie:

1. die Sicherheitsanwendungen von Kaspersky gemäß dem Szenario zur Verteilung von Kaspersky-Programmen via Kaspersky Security Center 14 Web Console auf den verwalteten Geräten verteilt haben.
2. alle notwendigen Richtlinien, Richtlinienprofile und Aufgaben entsprechend dem Szenario "Konfiguration des Netzwerkschutzes" konfiguriert haben.
3. in Übereinstimmung mit der Anzahl der verwalteten Geräte und der Netzwerktopologie eine geeignete Anzahl an Verteilungspunkten zugewiesen haben.

Das Update der Datenbanken und Programme von Kaspersky erfolgt in mehreren Etappen:

1. **Auswählen eines Update-Schemas**

   Es existieren verschiedene Schemen die Sie nutzen können, um Updates für die Komponenten des Kaspersky Security Centers und Sicherheitsanwendungen zu installieren. Wählen Sie ein Schema oder mehrere Schemen, welche die Anforderungen Ihres Netzwerks am besten erfüllen.

2. **Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen**

   Diese Aufgabe wird automatisch vom Schnellstartassistenten für Kaspersky Security Centers erstellt. Wenn Sie den Assistenten nicht ausgeführt haben, erstellen Sie die Aufgabe jetzt.

   Diese Aufgabe wird benötigt, um Updates von den Kaspersky-Update-Servern in die Datenverwaltung des Administrationsservers zu laden, und um die Updates der Kaspersky-Datenbanken und Programm-Module des Kaspersky Security Centers auszuführen. Nachdem die Updates heruntergeladen wurden, können Sie an die verwalteten Geräte weitergegeben werden.

   Wenn Ihr Netzwerk über zugewiesene Verteilungspunkte verfügt, werden die Updates aus der Datenverwaltung des Administrationsservers in die Datenverwaltungen der Verteilungspunkte geladen. In diesem Fall laden die verwalteten Geräte, die sich im Bereich eines Verteilungspunktes befinden, die Updates aus der Datenverwaltung des Verteilungspunktes, anstatt aus der Datenverwaltung des Administrationsservers.

   Anleitungen: Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen

3. **Aufgabe zum Download von Updates in die Datenverwaltung auf Verteilungspunkte erstellen (optional)**

   Standardmäßig werden die Updates von den Verteilungspunkten vom Administrationsserver heruntergeladen. Sie können Kaspersky Security Center so konfigurieren, dass die Verteilungspunkte die Updates direkt von den Kaspersky-Update-Servern herunterladen. Der direkte Download in die Datenverwaltung der Verteilungspunkte ist dann vorzuziehen, wenn der Datenverkehr zwischen dem Administrationsserver und den Verteilungspunkten teurer ist als der Datenverkehr zwischen den Verteilungspunkten und den Kaspersky-Update-Servern, oder wenn Ihr Administrationsserver keinen Internetzugang hat.

   Wenn Ihr Netzwerk über zugewiesene Verteilungspunkte verfügt und die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* erstellt wurde, laden die Verteilungspunkte Updates von den Kaspersky-Update-Servern herunter, und nicht von der Datenverwaltung des Administrationsservers.

   Anleitung: Aufgabe für den Download von Updates in die Datenverwaltung der Verteilungspunkte erstellen

4. **Konfigurieren der Verteilungspunkte**

   Wenn Ihr Netzwerk über zugewiesene Verteilungspunkte verfügt, stellen Sie sicher, dass die Option **Updates verteilen** in den Einstellungen aller benötigten Verteilungspunkte aktiviert ist. Wenn diese Option für einen Verteilungspunkt deaktiviert ist, laden die Geräte, die sich im Bereich dieses Verteilungspunktes befinden, die Updates von der Datenverwaltung des Administrationsservers herunter.

5. **Optimieren des Update-Vorgangs durch Diff-Dateien (optional)**

   Sie können den Datenverkehr zwischen dem Administrationsserver und den verwalteten Geräten optimieren, indem Sie Diff-Dateien verwenden. Wenn diese Funktion aktiviert ist, laden der Administrationsserver oder ein Verteilungspunkt im Gegensatz zu ganzen Kaspersky-Datenbank-Dateien oder Programm-Modulen nur Diff-Dateien herunter. Eine Diff-Datei beschreibt den Unterschied zwischen zwei Versionen der Datei einer Datenbank oder eines Programm-Moduls. Deswegen benötigt eine Diff-Datei weniger Platz als eine ganze Datei. Dies resultiert in einem verringerten Datenverkehr zwischen dem Administrationsserver oder Verteilungspunkt und den verwalteten Geräten. Um diese Funktion zu nutzen, aktivieren Sie die Option **Diff-Dateien herunterladen** in den Eigenschaften der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und/oder der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*.

   Anleitung: Diff-Dateien zum Update von Kaspersky-Datenbanken und Programm-Modulen verwenden

6. **Konfiguration der automatischen Installation von Updates für die Sicherheitsanwendungen**

Erstellen Sie die *Update*-Aufgaben für verwaltete Programme, um zeitnahe Updates für die Programm-Module und Kaspersky-Datenbanken (einschließlich der Antiviren-Datenbanken) zu gewährleisten. Damit Updates immer rechtzeitig erfolgen, sollten Sie beim Konfigurieren des Aufgabenplans die Option **Nach dem Download von Updates in die Datenverwaltung** aktivieren.

Wenn Ihr Netzwerk ausschließlich IPv6-Geräte enthält und Sie die auf den Geräten installierten Sicherheitsanwendungen regelmäßig aktualisieren möchten, stellen Sie sicher, das auf den verwalteten Geräten der Administrationsserver Version 13.2 und der Administrationsagent Version 13.2 installiert sind.

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.

Ergebnisse

Nach Abschluss des Szenarios ist Kaspersky Security Center Linux so konfiguriert, dass die Kaspersky-Datenbanken aktualisiert werden, nachdem die Updates in die Datenverwaltung des Administrationsservers heruntergeladen wurden. Anschließend können Sie mit der Überwachung des Netzwerkstatus fortfahren.

Informationen zum Aktualisieren von Kaspersky-Datenbanken, Softwaremodulen und Anwendungen

Um sicherzustellen, dass der Schutz Ihrer Administrationsserver und verwalteten Geräte auf dem neuesten Stand ist, müssen Sie zeitnah Updates bereitstellen für:

- Kaspersky-Datenbanken und Programm-Module

  Vor dem Herunterladen von Kaspersky-Datenbanken und Softwaremodulen überprüft Kaspersky Security Center, ob die Kaspersky-Server erreichbar sind. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet das Programm öffentliches DNS. 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 des Kaspersky Security Centers und der Sicherheitsanwendungen

  Kaspersky Security Center kann Kaspersky-Apps nicht automatisch aktualisieren. Um die Apps zu aktualisieren, laden Sie die neuesten App-Versionen von der Kaspersky-Website herunter und installieren Sie sie manuell:

  - Kaspersky Security Center Administrationsserver, Kaspersky Security Center 14 Web Console
  - Administrationsagent, Kaspersky Endpoint Security für Linux, Verwaltungs-Web-Plug-in

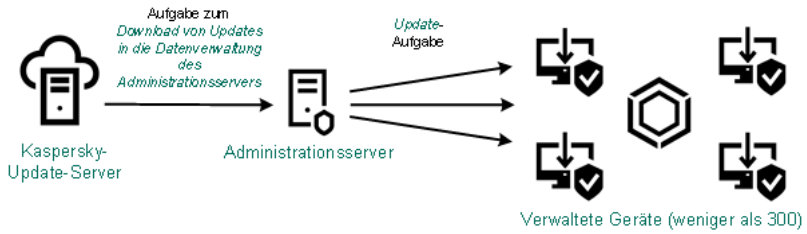
Abhängig von der Konfiguration Ihres Netzwerks können Sie die folgenden Schemata für das Herunterladen und Verteilen der erforderlichen Updates auf die verwalteten Geräte verwenden:

- Durch Verwendung einer einzelnen Aufgabe: *Download von Updates in die Datenverwaltung des Administrationsservers*
- Durch Verwendung zweier Aufgaben:
  - Die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*
  - Die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*

- Manuell über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server
- Direkt von den Kaspersky-Update-Servern an Kaspersky Endpoint Security für Linux auf den verwalteten Geräten
- Über einen lokalen Ordner oder Netzwerkordner, wenn der Administrationsserver keine Internetverbindung hat

Verwenden der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers

In diesem Schema lädt Kaspersky Security Center über die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* Updates herunter. In kleinen Netzwerken, die weniger als 300 verwaltete Geräte in einem einzelnen Netzwerksegment oder weniger als 10 verwaltete Geräte in jedem Netzwerksegment enthalten, werden die Updates direkt aus der Datenverwaltung des Administrationsservers auf die verwalteten Geräte verteilt (siehe Abbildung unten).



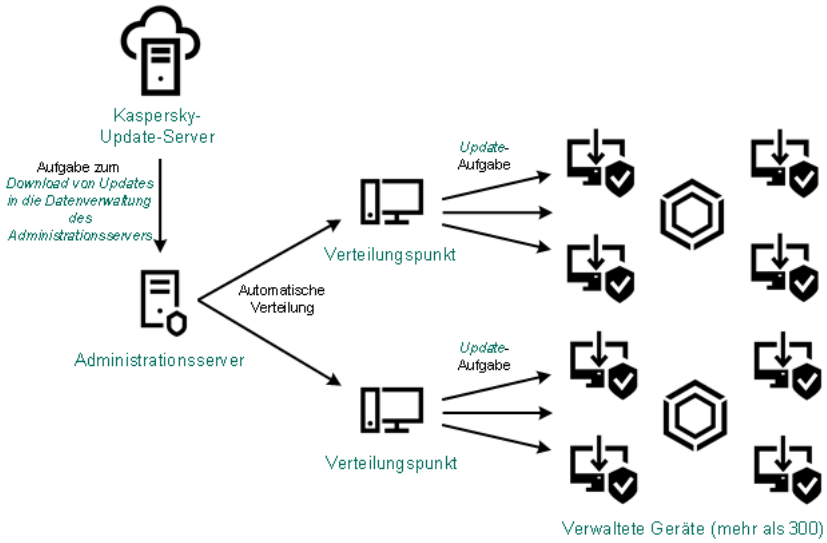
Update mithilfe der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers ohne Verteilungspunkte

Sie können nicht nur die Kaspersky-Update-Server als Update-Quelle verwenden, sondern auch einen lokalen Ordner oder einen Netzwerkordner.

Standardmäßig verwendet der Administrationsserver zur Kommunikation mit den Kaspersky-Update-Servern und zum Download von Updates das HTTPS-Protokoll. Sie können Administrationsserver so einrichten, dass das HTTP-Protokoll anstelle des HTTPS-Protokolls verwendet wird.

Wenn Ihr Netzwerk 300 oder mehr verwaltete Geräte in einem einzigen Netzwerksegment enthält oder wenn Ihr Netzwerk aus mehreren Netzwerksegmenten mit mehr als 9 verwalteten Geräten in jedem Netzwerksegment besteht, empfehlen wir Ihnen, Verteilungspunkte zu verwenden, um die Updates auf die verwalteten Geräte zu übertragen (siehe Abbildung unten). Verteilungspunkte reduzieren die Belastung des Administrationsservers und optimieren den Datenverkehr zwischen dem Administrationsserver und den verwalteten Geräten. Sie können die Anzahl und Konfiguration der für Ihr Netzwerk benötigten Verteilungspunkte berechnen.

In diesem Schema werden die Updates automatisch aus der Datenverwaltung des Administrationsservers in die Datenverwaltungen der Verteilungspunkte heruntergeladen. Die verwalteten Geräte, die zum Umfang eines Verteilungspunkts gehören, laden die Updates aus der Datenverwaltung des Verteilungspunkts anstelle der Datenverwaltung des Administrationsservers herunter.



Update mithilfe der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers mit Verteilungspunkten

Nach Abschluss der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* werden die Updates für die Kaspersky-Datenbanken und die Programm-Module für Kaspersky Endpoint Security für Linux in die Datenverwaltung des Administrationsservers heruntergeladen. Diese Updates werden über die Update-Aufgabe für Kaspersky Endpoint Security für Linux installiert.

Die Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers steht auf virtuellen Administrationsservern nicht zur Verfügung. In der Datenverwaltung des virtuellen Administrationsservers werden Updates angezeigt, die auf den primären Administrationsserver heruntergeladen wurden.

Sie können die Updates, die auf Funktionsfähigkeit und Fehler geprüft werden sollen, auf einer Reihe von Testgeräten konfigurieren. Wenn die Überprüfung erfolgreich ist, werden die Updates an andere verwaltete Geräte verteilt.

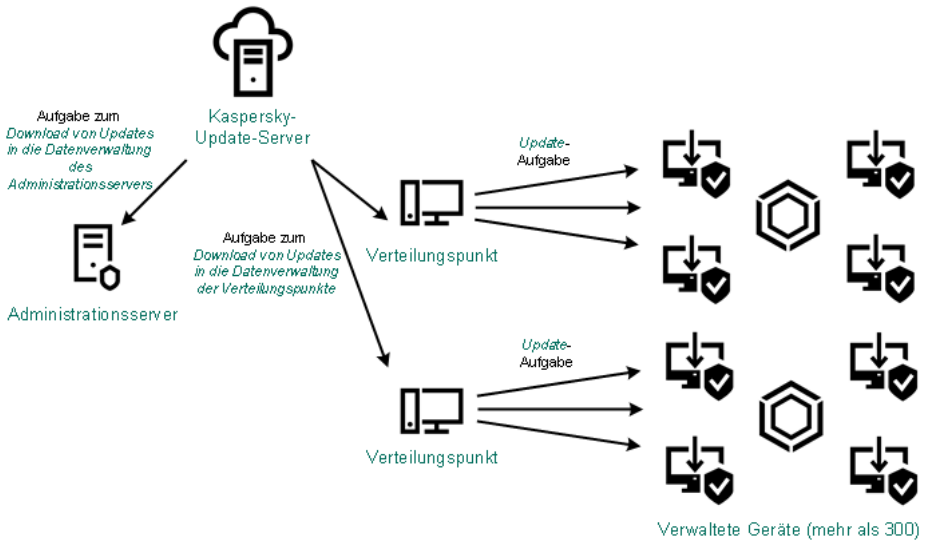
Jede Anwendung von Kaspersky fordert die erforderlichen Updates vom Administrationsserver an. Der Administrationsserver aggregiert diese Anforderungen und lädt nur die Aktualisierungen herunter, die von einer Anwendung angefordert werden. Dadurch wird sichergestellt, dass die gleichen Updates nicht mehrmals heruntergeladen werden und unnötige Updates überhaupt nicht heruntergeladen werden. Bei der Ausführung der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* der Administrationsserver die folgenden Informationen automatisch an Kaspersky-Update-Server, um das Herunterladen von relevanten Versionen der Kaspersky-Datenbanken und Programm-Module sicherzustellen:

- Anwendungs-ID und Version des Programms
- Programm-Setup-ID
- ID des aktiven Schlüssels
- Ausführungs-ID der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*

Keine der übermittelten Informationen enthält persönliche oder andere vertrauliche Daten. AO Kaspersky Lab schützt die erhaltenen Informationen in Übereinstimmung mit den geltenden gesetzlich festgelegten Anforderungen.

Verwendung von zwei Aufgaben: Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers und Aufgabe Updates in die Datenverwaltung der Verteilungspunkte herunterladen

Sie können Updates für die Datenverwaltungen der Verteilungspunkte direkt von den Update-Servern von Kaspersky anstelle der Datenverwaltung des Administrationsservers herunterladen und die Updates dann auf die verwalteten Geräte verteilen (siehe Abbildung unten). Der direkte Download in die Datenverwaltung der Verteilungspunkte ist dann vorzuziehen, wenn der Datenverkehr zwischen dem Administrationsserver und den Verteilungspunkten teurer ist als der Datenverkehr zwischen den Verteilungspunkten und den Kaspersky-Update-Servern, oder wenn Ihr Administrationsserver keinen Internetzugang hat.



Update mithilfe der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers und der Aufgabe Updates in die Datenverwaltung der Verteilungspunkte herunterladen

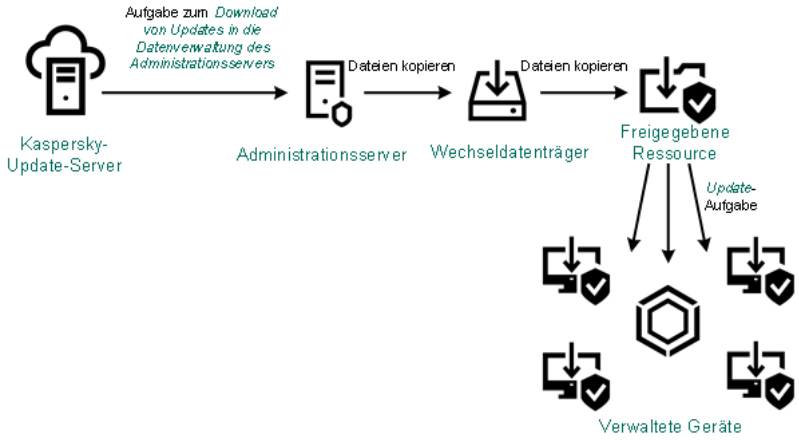
Standardmäßig verwenden der Administrationsserver und die Verteilungspunkte zur Kommunikation mit den Kaspersky-Update-Servern und zum Download von Updates das HTTPS-Protokoll. Sie können den Administrationsserver und/oder die Verteilungspunkte so konfigurieren, dass das HTTP-Protokoll anstelle des HTTPS-Protokolls verwendet wird.

Um dieses Schema zu implementieren, erstellen Sie die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* zusätzlich zur Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*. Danach laden die Verteilungspunkte die Updates von den Kaspersky Update-Servern herunter und nicht von der Datenverwaltung des Administrationsservers.

Die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* wird auch für dieses Schema benötigt, da mit dieser Aufgabe Datenbanken und Softwaremodule von Kaspersky für das Kaspersky Security Center heruntergeladen werden können.

Manuell über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server

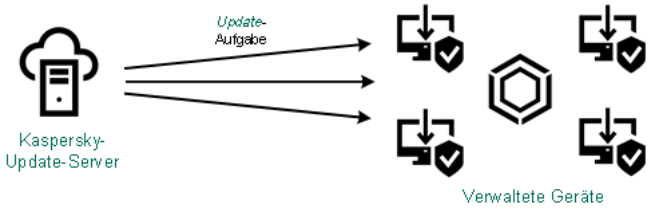
Wenn die Client-Geräte keine Verbindung zum Administrationsserver haben, können Sie einen lokalen Ordner oder eine freigegebene Ressource als Quelle für das Update von Kaspersky-Datenbanken, -Softwaremodulen und -Anwendungen verwenden. In diesem Schema müssen Sie die erforderlichen Updates aus der Datenverwaltung des Administrationsservers auf einen Wechseldatenträger kopieren und dann in den lokalen Ordner oder die als Update-Quelle in den Einstellungen von Kaspersky Endpoint Security für Linux angegebene freigegebene Ressource (siehe Abbildung unten).



Manuelles Upgrade über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server

Direkt von den Kaspersky-Update-Servern an Kaspersky Endpoint Security für Linux auf den verwalteten Geräten

Auf den verwalteten Geräten können Sie Kaspersky Endpoint Security für Linux 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 bereitgestellte Datenverwaltung. Um Updates direkt von den Kaspersky-Update-Servern zu erhalten, geben Sie in der Sicherheits-App die Kaspersky-Update-Server als Update-Quelle an. Eine vollständige Beschreibung der Einstellungen finden Sie in der Dokumentation zu Kaspersky Endpoint Security für Linux.

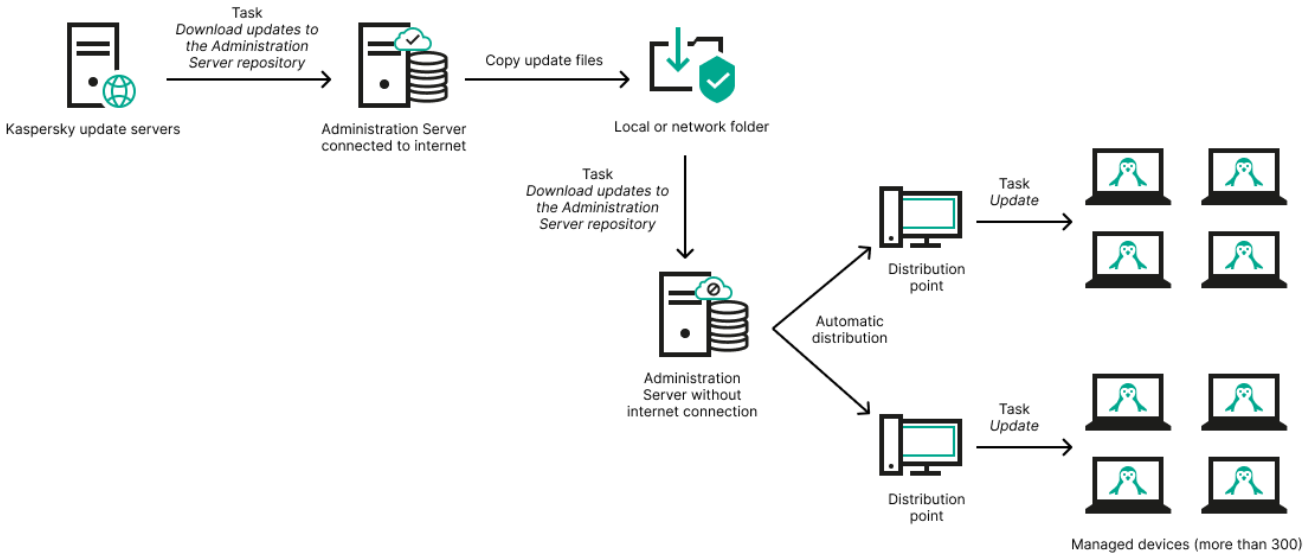
Über einen lokalen Ordner oder Netzwerkordner, wenn der Administrationsserver keine Internetverbindung hat

Wenn der Administrationsserver keine Internetverbindung hat, können Sie die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* zum Herunterladen von Updates aus einem lokalen oder Netzwerkordner konfigurieren. In diesem Fall müssen Sie die erforderlichen Update-Dateien von Zeit zu Zeit in den angegebenen Ordner kopieren. Beispielsweise können Sie die erforderlichen Update-Dateien aus einer der folgenden Quellen kopieren:

- Administrationsserver mit Internetverbindung (siehe Abbildung unten)

  Da ein Administrationsserver nur die Updates herunterlädt, die von den Sicherheitsanwendungen angefordert werden, müssen die Gruppen der Sicherheitsanwendungen, die von den Administrationsservern verwaltetet werden – d. h. von dem mit Internetverbindung und dem ohne Internetverbindung – übereinstimmen.

  Wenn der von Ihnen zum Herunterladen von Updates verwendete Administrationsserver die Version 13.2 besitzt, öffnen Sie die Eigenschaften der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und aktivieren Sie anschließend die Option **Updates nach altem Schema herunterladen**.



Aktualisieren mittels eines lokalen Ordners oder Netzwerkordners, wenn der Administrationsserver keine Internetverbindung hat

- Kaspersky Update Utility

  Da dieses Tool das alte Schema zum Herunterladen von Updates verwendet, öffnen Sie die Eigenschaften der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und aktivieren Sie anschließend die Option *Updates nach altem Schema herunterladen*.

Die Aufgabe "Download von Updates in die Datenverwaltung des Administrationsservers" erstellen

Die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ist erforderlich, um die Updates für Datenbanken und Programm-Module von Kaspersky-Sicherheitsanwendungen von den Kaspersky-Update-Servern in die Administrationsserver-Datenverwaltung herunterzuladen.

Der Schnellstartassistent von Kaspersky Security Center erstellt automatisch die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* für den Administrationsserver. In der Aufgabenliste kann nur eine Aufgabe des Typs *Download von Updates in die Datenverwaltung des Administrationsservers* vorhanden sein. Sie können diese Aufgabe erneut erstellen, wenn sie aus der Aufgabenliste des Administrationsservers entfernt wurde.

Nachdem die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* abgeschlossen und die Updates heruntergeladen wurden, können diese an die verwalteten Geräte weitergegeben werden.

> Bevor Sie Updates an die verwalteten Geräte weiterleiten, können Sie die Aufgabe zur *Update-Prüfung* ausführen. Dadurch können Sie sicherstellen, dass der Administrationsserver die heruntergeladenen Updates ordnungsgemäß installiert und die Sicherheitsstufe durch etwaige Updates nicht verringert wird. Um sie vor dem Verteilen zu überprüfen, konfigurieren Sie die Option **Update-Prüfung ausführen** in den Einstellungen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*.

Um die Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers zu erstellen:

1. Gehen Sie 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 den Aufgabentyp **Download von Updates in die Datenverwaltung des Administrationsservers**.

4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.

5. Auf der Seite **Erstellung der Aufgabe abschließen** können Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktivieren, um das Fenster mit den Aufgabeneigenschaften zu öffnen und die Aufgabeneinstellungen zu ändern. Alternativ können Sie Aufgabeneinstellungen jederzeit später konfigurieren.

6. Klicken Sie auf die Schaltfläche **Fertigstellen**.

   Die Aufgabe wird erstellt und in der Aufgabenliste angezeigt.

7. Um das Fenster mit den Aufgabeneigenschaften zu öffnen, klicken Sie auf den Namen der erstellten Aufgabe.

8. Geben Sie im Fenster mit den Aufgabeneigenschaften auf der Registerkarte **Programmeinstellungen** die folgenden Einstellungen an:

   - **Update-Quellen**

     Sie können als Update-Quelle die Kaspersky-Update-Server, einen lokalen oder Netzwerkordner oder einen primären Administrationsserver verwenden.

   - **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.

   - **Heruntergeladene Updates in zusätzliche Ordner kopieren**

     Nachdem der Administrationsserver Updates empfängt, kopiert er sie in die angegebenen Ordner. Verwenden Sie diese Option, wenn Sie die Verteilung von Updates in Ihrem Netzwerk manuell verwalten möchten.

     Sie können diese Option beispielsweise in der folgenden Situation verwenden: Das Netzwerk Ihres Unternehmens besteht aus mehreren unabhängigen Subnetzen, wobei Geräte in den einzelnen Subnetzen über keinen Zugriff auf andere Subnetze verfügen. Allerdings haben Geräte in allen Teilnetzen Zugriff auf eine gemeinsame Netzwerkfreigabe. In diesem Fall müssen Sie den Administrationsserver in einem der Subnetze einrichten, um Updates von den Kaspersky-Update-Servern herunterzuladen. Aktivieren Sie diese Option und geben Sie dann diese Netzwerkfreigabe an. Geben Sie bei heruntergeladenen Updates der Repository-Aufgaben für andere Administrationsserver die gleiche Netzwerkfreigabe wie für die Update-Quelle an.

     Diese Option ist standardmäßig deaktiviert.

   - **Diff-Dateien herunterladen**

     Diese Option aktiviert die Funktion zum Download von Diff-Dateien.

     Diese Option ist standardmäßig deaktiviert.

   - **Updates nach altem Schema herunterladen**

Ab Version 14 lädt Kaspersky Security Center die Updates von Datenbanken und Softwaremodulen unter Verwendung eines neuen Schemas herunter. Damit das Programm die Updates mithilfe des neuen Schemas herunterladen kann, muss die Updatequelle die Update-Dateien mit den Metadaten enthalten, die mit dem neuen Schema kompatibel sind. Wenn die Updatequelle 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 Updatequelle 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

  Beispiel: Ihr Administrationsserver 1 besitzt keine Internetverbindung. In diesem Fall können Sie Updates über einen Administrationsserver 2 herunterladen, welcher über eine Internetverbindung verfügt, und welcher die Updates anschließend in einem lokalen Ordner oder Netzwerkordner ablegt. Dieser dient wiederum als Updatequelle für den Administrationsserver 1. Wenn der Administrationsserver 2 mit Version 13.2 oder früher läuft, aktivieren Sie die Option **Updates nach altem Schema herunterladen** in der Aufgabe für Administrationsserver 1.

Diese Option ist standardmäßig deaktiviert.

- **Update-Prüfung ausführen**

  Der Administrationsserver lädt Updates von der Quelle herunter, speichert sie in einer temporären Datenverwaltung und führt die Aufgabe aus, die im Feld **Aufgabe zur Update-Prüfung** angegeben wurde. Wenn die Aufgabe erfolgreich beendet wird, werden die Updates von der temporären Datenverwaltung in einen freigegebenen Ordner auf dem Administrationsserver kopiert und anschließend auf alle Geräte verteilt, für die der Administrationsserver als Update-Quelle dient (Aufgaben mit dem Zeitplantyp **Nach dem Download von Updates in die Datenverwaltung** werden gestartet). Die Aufgabe zum Download von Updates in die Datenverwaltung wird erst nach Abschluss der Aufgabe zur *Update-Prüfung* beendet.

  Diese Option ist standardmäßig deaktiviert.

9. Erstellen Sie im Fenster mit den Aufgabeneigenschaften auf der Registerkarte **Zeitplan** einen Zeitplan für den Aufgabenstart. Geben Sie erforderlichenfalls die folgenden Einstellungen an:

   - **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 Abwärtskompatibilität von Kaspersky Security Center Linux 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 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.

- Weitere Aufgabeneinstellungen:

  - **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.

- **Aufgabe anhalten, wenn Aufgabe länger ausgeführt wird als (Min.)**

  Nachdem die festgelegte Zeitspanne abgelaufen ist, wird die Aufgabe automatisch angehalten, egal ob sie abgeschlossen ist oder nicht.

  Aktivieren Sie diese Option, wenn Sie Aufgaben, deren Ausführung zu lange dauert, unterbrechen (oder anhalten) möchten.

  Diese Option ist standardmäßig deaktiviert. Die Standardzeit für die Aufgabenausführung beträgt 120 Minuten.

10. Klicken Sie auf die Schaltfläche **Speichern**.

    Die Aufgabe wird erstellt und konfiguriert.

Nach Fertigstellung der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* werden die Datenbanken-Updates und Updates der Programm-Module von der Update-Quelle geladen und im freigegebenen Ordner des Administrationsservers gespeichert. Wenn die Aufgabe für eine Administrationsgruppe erstellt wird, kommt sie nur auf Administrationsagenten zur Anwendung, die zur angegebenen Administrationsgruppe gehören.

Updates werden aus dem gemeinsamen Ordner des Administrationsservers an Client-Geräte und sekundäre Administrationsserver verteilt.

Heruntergeladene Updates anzeigen

Nach Fertigstellung der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* werden die Datenbanken-Updates und Updates der Programm-Module von der Update-Quelle geladen und im freigegebenen Ordner des Administrationsservers gespeichert. Sie können die heruntergeladenen Updates im Abschnitt **UPDATES FÜR KASPERSKY-DATENBANKEN UND -SOFTWAREMODULE** einsehen.

Um die Liste der heruntergeladenen Updates anzusehen,

Wechseln Sie im Hauptmenü zu **VORGÄNGE → PROGRAMME VON KASPERSKY → UPDATES FÜR KASPERSKY-DATENBANKEN UND -SOFTWAREMODULE**.

Eine Liste verfügbarer Updates wird geöffnet.

Heruntergeladene Updates prüfen

Bevor Sie Updates auf den verwalteten Geräten installieren, können Sie die Updates zunächst über die Aufgabe zur *Update-Prüfung* auf Funktionsfähigkeit und Fehler überprüfen. Die Aufgabe zur *Update-Prüfung* wird automatisch im Rahmen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ausgeführt. Der Administrationsserver lädt Updates aus der Quelle herunter, speichert sie in einem temporären Verzeichnis und startet die Aufgabe zur *Update-Prüfung*. Wenn die Aufgabe erfolgreich ausgeführt wurde, werden die Updates von der temporären Datenverwaltung in den freigegebenen Ordner des Administrationsservers kopiert. Sie werden an alle Client-Geräte verteilt, für die der Administrationsserver als Update-Quellen dient.

Wenn in den Ergebnissen der Aufgabe zur *Update-Prüfung* die im temporären Verzeichnis liegenden Updates als fehlerhaft eingestuft werden oder wenn die Aufgabe zur *Update-Prüfung* mit einem Fehler beendet wird, werden die Updates nicht im freigegebenen Ordner gespeichert. Auf dem Administrationsserver verbleibt das vorherige Update. Dann werden auch die Aufgaben mit dem Zeitplantyp **Nach dem Download von Updates in die Datenverwaltung** nicht gestartet. Diese Vorgänge werden beim nächsten Ausführen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* gestartet, wenn die Prüfung der neuen Updates erfolgreich verläuft.

Das Update gilt als fehlerhaft, wenn mindestens ein Testgerät eine der folgenden Bedingungen erfüllt:

- Es ist ein Fehler in einer Update-Aufgabe aufgetreten.
- Nach Übernahme der Updates hat sich der Status des Echtzeitschutzes der Sicherheitsanwendung geändert.
- Während der Ausführung der Untersuchungsaufgabe auf Befehl wurde ein infiziertes Objekt gefunden.
- Es ist ein Funktionsfehler im Kaspersky-Programm aufgetreten.

Wenn auf keinem Testgerät eine der genannten Bedingungen erfüllt wurde, wird das Set an Updates als ordnungsgemäß anerkannt und die Aufgabe zur *Update-Prüfung* gilt als erfolgreich abgeschlossen.

Bevor Sie mit der Erstellung der Aufgabe zur *Update-Prüfung* beginnen, führen Sie folgende Voraussetzungen aus:

1. Erstellen Sie eine Administrationsgruppe mit mehreren Testgeräten. Sie benötigen diese Gruppe, um die Updates zu prüfen.

   Es wird empfohlen Testgeräte zu verwenden, die gut geschützt sind und die eine Programmkonfiguration aufweisen, die im Unternehmensnetzwerk am weitesten verbreitet ist. Dieser Ansatz erhöht während der Untersuchung die Qualität und Wahrscheinlichkeit der Entdeckung von Viren und minimiert das Risiko von Fehlalarmen. Wenn Viren auf Testgeräten gefunden werden, wird die Aufgabe zur *Update-Prüfung* als nicht erfolgreich betrachtet.

2. Erstellen Sie die Update-Aufgabe und die Aufgabe zur Untersuchung auf Viren für ein von Kaspersky Security Center unterstütztes Programm, z. B. Kaspersky Endpoint Security für Linux. Geben Sie beim Erstellen der Update-Aufgabe und der Aufgabe zur Untersuchung auf Viren die Administrationsgruppe mit den Testgeräten an.

   Die Aufgabe zur *Update-Prüfung* führt die Update-Aufgabe und die Aufgabe zur Untersuchung auf Viren auf den Testgeräten nacheinander aus, um zu überprüfen, ob alle Updates zulässig sind. Beim Erstellen der Aufgabe zur *Update-Prüfung*, müssen Sie zusätzlich die Update-Aufgabe und die Aufgabe zur Untersuchung auf Viren angeben.

3. Erstellen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*.

Damit Kaspersky Security Center Linux die empfangenen Updates überprüft, bevor sie auf die Client-Geräte verteilt werden:

1. Wechseln Sie im Hauptmenü zu **GERÄTE** → **AUFGABEN**.
2. Klicken Sie auf die Aufgabe **Download von Updates in die Datenverwaltung des Administrationsservers**.

3. Wechseln Sie im folgenden Fenster mit den Aufgabeneigenschaften zur Registerkarte **Programmeinstellungen** und aktivieren Sie anschließend die Option **Update-Prüfung ausführen**.

4. Wenn die Aufgabe zur *Update-Prüfung* existiert, klicken Sie auf die Schaltfläche **Aufgabe auswählen**. Wählen Sie im folgenden Fenster die Aufgabe zur *Update-Prüfung* in der Administrationsgruppe mit den Testgeräten aus.

5. Wenn Sie die Aufgabe zur *Update-Prüfung* noch nicht erstellt haben, gehen Sie wie folgt vor:

   a. Klicken Sie auf die Schaltfläche **Neue Aufgabe**.

   b. Geben Sie im folgenden Assistenten zum Hinzufügen von Aufgaben einen Aufgabennamen an, wenn Sie den voreingestellten Namen ändern möchten.

   c. Wählen Sie die zuvor erstellte Administrationsgruppe mit den Testgeräten aus.

   d. Wählen Sie für ein erforderliches Programms, das von Kaspersky Security Center unterstützt wird, zunächst die Update-Aufgabe und anschließend die Aufgabe zur Untersuchung auf Viren aus.

   Danach werden die folgenden Optionen angezeigt. Es wird empfohlen, diese aktiviert zu lassen:

   - **Gerät nach Datenbanken-Update neu starten**

     Nachdem die Antiviren-Datenbanken eines Gerät aktualisiert wurden, wird es empfohlen, das Gerät neu zu starten.

     Die Option ist standardmäßig aktiviert.

   - **Status des Echtzeitschutzes nach Datenbanken-Update und Geräteneustart überprüfen**

     Wenn diese Option aktiviert ist prüft die Aufgabe zur *Update-Prüfung*, ob die in die Datenverwaltung des Administrationsservers heruntergeladenen Updates zulässig sind und ob die Schutzstufe nach dem Update der Antiviren-Datenbanken und dem Neustart des Geräts gesunken ist.

     Diese Option ist standardmäßig aktiviert.

   e. Geben Sie ein Konto an, unter welchem die Aufgabe zur *Update-Prüfung* ausgeführt wird. Sie können Ihr Konto verwenden und die Option **Standardbenutzerkonto** aktiviert lassen. Alternativ können Sie angeben, dass die Aufgabe unter einem anderen Konto ausgeführt werden soll, welches über die erforderlichen Zugriffsrechte verfügt. Wählen Sie dazu die Option **Benutzerkonto festlegen** aus und geben Sie anschließend die Anmeldeinformationen für dieses Konto ein.

6. Klicken Sie auf **Speichern**, um das Eigenschaftenfenster der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* zu schließen.

Die automatische Update-Prüfung ist aktiviert. Wenn Sie jetzt die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ausführen, beginnt diese mit der Update-Prüfung.

Erstellen der Aufgabe für den Download von Updates in die Datenverwaltung der Verteilungspunkte

Sie können die Aufgabe zum *Download von Updates in die Datenverwaltung der Verteilungspunkte* für eine Administrationsgruppe erstellen. Diese Aufgabe wird für die Verteilungspunkte ausgeführt, die zur angegebenen Administrationsgruppe gehören.

Sie können diese Aufgabe zum Beispiel dann nutzen, wenn der Datenverkehr zwischen dem Administrationsserver und den Verteilungspunkten teurer ist als der Datenverkehr zwischen den Verteilungspunkten und den Kaspersky-Update-Servern, oder wenn Ihr Administrationsserver keinen Internetzugang hat.

Diese Aufgabe ist erforderlich, um Updates von Kaspersky-Update-Servern in die Datenverwaltung der Verteilungspunkte herunterzuladen. Die Liste der Updates enthält:

- Updates von Datenbanken und Softwaremodulen für Kaspersky-Sicherheitsanwendungen
- Updates der Kaspersky Security Centers-Komponenten
- Updates von Kaspersky-Sicherheitsanwendungen

Nachdem die Updates heruntergeladen wurden, können Sie an die verwalteten Geräte weitergegeben werden.

*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 zum Hinzufügen von Aufgaben wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie für Kaspersky Security Center im Feld **Aufgabentyp** die Option **Updates in die Datenverwaltung der Verteilungspunkte herunterladen**.
4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.
5. Wählen Sie eine Optionsschaltfläche, um die Administrationsgruppe, die Geräteauswahl oder die Geräte, für die Aufgabe gilt, festzulegen.
6. Wenn Sie im Schritt **Erstellung der Aufgabe abschließen** die Standardeinstellungen der Aufgabe ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.
7. Klicken Sie auf 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.

Wenn Sie die Option **Keinen Proxyserver verwenden** für die Updatequellen Kaspersky-Update-Server oder Lokaler Ordner oder Netzwerkordner aktiviert haben, verwendet ein Verteilungspunkt selbst dann keinen Proxy-Server für den Update-Download, wenn Sie in den Einstellungen des Administrationsagenten dieses Verteilungspunkts die Option **Proxyserver verwenden** aktiviert haben.

- **Ordner zum Speichern von Updates**

  Der Pfad zum angegebenen Ordner, in dem die bezogenen Updates gespeichert werden. Sie können den Pfad des angegebenen Ordners in die Zwischenablage kopieren. Für eine Gruppenaufgabe können Sie den Pfad eines angegebenen Ordners nicht ändern.

- **Diff-Dateien herunterladen**

  Diese Option aktiviert die Funktion zum Download von Diff-Dateien.

  Diese Option ist standardmäßig deaktiviert.

- **Updates nach altem Schema herunterladen**

Ab Version 14 lädt Kaspersky Security Center die Updates von Datenbanken und Softwaremodulen unter Verwendung eines neuen Schemas herunter. Damit das Programm die Updates mithilfe des neuen Schemas herunterladen kann, muss die Updatequelle die Update-Dateien mit den Metadaten enthalten, die mit dem neuen Schema kompatibel sind. Wenn die Updatequelle 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 Updatequelle 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 Abwärtskompatibilität von Kaspersky Security Center Linux 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.

- **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.

Hinzufügen von Update-Quellen für die Aufgabe "Download von Updates in die Datenverwaltung des Administrationsservers"

Wenn Sie die Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen oder verwenden, stehen die folgenden Update-Quellen zur Auswahl:

- Kaspersky-Update-Server
- Primärer Administrationsserver

  Diese Ressource gilt für Aufgaben, die für einen sekundären oder virtuellen Administrationsserver erstellt wurden.
- Lokaler Ordner oder Netzwerkordner

Die Kaspersky-Update-Server werden standardmäßig verwendet, Sie können die Updates jedoch auch aus einem lokalen Ordner oder Netzwerkordner herunterladen. Den Ordner können Sie beispielsweise verwenden, wenn Ihr Netzwerk keinen Internetzugriff hat. In diesem Fall können Sie die Updates manuell von den Kaspersky-Update-Servern herunterladen und die heruntergeladenen Dateien im erforderlichen Ordner ablegen.

Sie können nur einen Pfad für einen lokalen Ordner oder Netzwerkordner angeben. Als lokaler Ordner kommt nur einen Ordner auf dem Administrationsserver in Frage; Als Netzwerkordner können Sie nur einen FTP- oder HTTP-Server verwenden.

Wenn Sie sowohl die Kaspersky-Update-Server als auch den lokalen Ordner oder Netzwerkordner hinzufügen, werden die Updates zuerst aus dem Ordner heruntergeladen. Tritt beim Herunterladen ein Fehler auf, werden die Kaspersky-Update-Server verwendet.

Falls ein freigegebener Ordner mit Updates passwortgeschützt ist, aktivieren Sie die Option **Benutzerkonto für den Zugriff auf den freigegebenen Ordner der Update-Quelle angeben (falls vorhanden)** und geben Sie die für den Zugriff erforderlichen Anmeldeinformationen ein.

Um die Update-Quellen hinzuzufügen:

1. Gehen Sie zu **GERÄTE → AUFGABEN**.
2. Klicken Sie auf die Schaltfläche **Download von Updates in die Datenverwaltung des Administrationsservers**.
3. Gehen Sie zur Registerkarte **Programmeinstellungen**.
4. Klicken Sie in der Zeile **Update-Quellen** auf **Anpassen**.
5. Klicken Sie im folgenden Fenster auf **Hinzufügen**.
6. Fügen Sie in der Liste der Update-Quellen die erforderlichen Quellen hinzu. Wenn Sie das Kontrollkästchen **Lokaler Ordner oder Netzwerkordner** aktivieren, geben Sie einen Ordnerpfad an.
7. Klicken Sie auf **Uhrzeit der Verschlüsselung** und schließen Sie dann das Eigenschaftenfenster der Update-Quelle.
8. Klicken Sie im Fenster der Update-Quelle auf **Uhrzeit der Verschlüsselung**.
9. Klicken Sie im Aufgabenfenster auf **Speichern**.

Jetzt werden Updates aus den angegebenen Quellen in die Datenverwaltung des Administrationsservers heruntergeladen.

Über die Verwendung von Diff-Dateien zum Update von Kaspersky-Datenbanken und Software-Modulen

Beim Update-Download von den Kaspersky-Update-Servern optimiert Kaspersky Security Center den Datenverkehr durch die Verwendung von Diff-Dateien. Sie können festlegen, dass Geräte (Administrationsserver, Verteilungspunkte, Client-Geräte), die Updates von anderen Geräten in Ihrem Netzwerk erhalten, ebenfalls Diff-Dateien verwenden.

Über die Funktion zum Download von Diff-Dateien

Eine Diff-Datei beschreibt den Unterschied zwischen zwei Versionen der Datei einer Datenbank oder eines Programm-Moduls. Die Verwendung von Diff-Dateien entlastet den Datenverkehr in Ihrem Unternehmensnetzwerk, da Diff-Dateien weniger Platz einnehmen als die vollständigen Dateien der Datenbanken und Software-Module. Wenn die Funktion *Diff-Dateien herunterladen* auf dem Administrationsserver oder dem Verteilungspunkt aktiviert ist, werden die Diff-Dateien auf diesem Administrationsserver oder Verteilungspunkt gespeichert. So können Geräte, die Updates vom Administrationsserver oder einem Verteilungspunkt erhalten, die gespeicherten Diff-Dateien verwenden, um ihre Datenbanken und Software-Module zu aktualisieren.

Um die Verwendung von Diff-Dateien zu optimieren, wird empfohlen, den Update-Zeitplan der Geräte mit dem Update-Zeitplan des Administrationsservers oder dem Verteilungspunkt, von denen sie ihre Updates erhalten, zu synchronisieren. Der Datenverkehr kann jedoch auch dann reduziert werden, wenn die Geräte viel seltener aktualisiert werden als der Administrationsserver oder der Verteilungspunkt, von dem sie ihre Updates erhalten.

Verteilungspunkte verwenden kein IP-Multicast zur automatischen Verteilung von Diff-Dateien.

Aktivieren der Funktion zum Downloaden von Diff-Dateien: Szenario

Schritte

1. **Aktivieren der Funktion auf dem Administrationsserver**

   Aktivieren Sie die Funktion in den Einstellungen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*.

2. **Aktivieren der Funktion für einen Verteilungspunkt**

   Aktivieren Sie die Funktion für Verteilungspunkte, die Updates mithilfe der Aufgabe *Download von Updates in die Datenverwaltung der Verteilungspunkte* erhalten.

   Aktivieren Sie anschließend in den Einstellungen Richtlinie des Administrationsagenten die Funktion für die Verteilungspunkte, die Updates vom Administrationsserver erhalten.

   Aktivieren Sie anschließend die Funktion für Verteilungspunkte, die Updates vom Administrationsserver erhalten.

   Die Funktion wird in den Einstellungen des Administrationsagenten und – falls die Verteilungspunkte manuell zugewiesen werden und Sie die Einstellungen der Richtlinie überbrücken möchten – im Abschnitt **Verteilungspunkte** in den Eigenschaften des Administrationsservers aktiviert.

Um zu prüfen, ob die Funktion zum Download von Diff-Dateien erfolgreich aktiviert wurde, können Sie den internen Datenverkehr vor und nach der Implementierung des Szenarios messen.

Updates über Verteilungspunkte empfangen

In Kaspersky Security Center Linux können die Verteilungspunkte Updates vom Administrationsserver, von den Servern von Kaspersky, aus lokalen oder Netzwerkordnern abrufen.

Um den Update-Download für den Verteilungspunkt anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptfenster der Anwendung neben dem Namen des benötigten Administrationsservers auf das Symbol **Einstellungen** ( ).

   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, über den Updates an die Client-Geräte in der Gruppe verteilt werden.

4. Wählen Sie im Eigenschaftenfenster des Verteilungspunkts den Abschnitt **Update-Quelle** aus.

5. Wählen Sie die Update-Quelle für den Verteilungspunkt:

   - Update-Quelle

Wählen Sie eine Update-Quelle für den Verteilungspunkt aus:

- Damit der Verteilungspunkt die Updates vom Administrationsserver erhält, wählen Sie **Vom Administrationsserver beziehen**.
- Damit Verteilungspunkte Updates anhand einer Aufgabe beziehen können, wählen Sie **Aufgaben zum Update-Download verwenden** aus und geben Sie anschließend eine Aufgabe vom Typ *Download von Updates in die Datenverwaltung der Verteilungspunkte* an:
  - Wenn eine solche Aufgabe bereits auf dem Gerät vorhanden ist, wählen Sie die Aufgabe in der Liste aus.
  - Wenn auf dem Gerät noch keine derartige Aufgabe vorhanden ist, klicken Sie auf den Link **Aufgabe erstellen**, um eine Aufgabe zu erstellen. Der Assistent zum Hinzufügen von Aufgaben wird gestartet. Folgen Sie den Anweisungen des Assistenten.

- **Diff-Dateien herunterladen**

  Diese Option aktiviert die Funktion zum Download von Diff-Dateien.

  Diese Option ist standardmäßig aktiviert.

Daraufhin bezieht der Verteilungspunkt die Updates von der angegebenen Quelle.

Update der Kaspersky-Datenbanken und Programm-Module auf autonomen Geräten

Das Durchführen von Updates der Kaspersky-Datenbanken und Programm-Module ist eine wichtige Aufgabe, um den Schutz gegen Viren und andere Bedrohungen aufrechtzuerhalten. In der Regel konfigurieren Administratoren regelmäßige Updates durch die Nutzung der Datenverwaltungen des Administrationsservers.

Wenn Sie Updates von Datenbanken und Programm-Modulen auf einem Gerät (oder auf einer Gruppe von Geräten) durchführen müssen, die nicht mit dem Administrationsserver (primär oder sekundär), einem Verteilungspunkt oder dem Internet verbunden sind, müssen Sie eine alternative Update-Quelle, wie einen FTP-Server oder einen lokalen Ordner, nutzen. In diesem Fall müssen Sie die für die Updates benötigten Dateien über ein Massenspeichergerät, wie beispielsweise ein USB-Stick oder eine externe Festplatte, bereitstellen.

Kopieren Sie die benötigten Updates vom:

- Administrationsserver.

  Um sicherzustellen, dass die Datenverwaltung des Administrationsservers über die, von der auf dem autonomen Gerät installierten Sicherheitsanwendung benötigten, Updates verfügt, muss auf mindestens einem der verwalteten Online-Geräte die gleiche Sicherheitsanwendung installiert sein. Dieses Programm muss so angepasst sein, dass es mithilfe der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* die Updates aus der Administrationsserver-Datenverwaltung erhält.

- Jedes Gerät, dass die gleiche Sicherheitsanwendung installiert und so konfiguriert hat, dass sie Updates aus den Datenverwaltungen des Administrationsservers oder der Verteilungspunkte, oder direkt von den Kaspersky-Servern erhält.

Unten befindet sich ein Beispiel zur Update-Konfiguration von Datenbanken und Programm-Modulen, in welcher die Updates aus der Datenverwaltung des Administrationsservers kopiert werden.

So aktualisieren Sie Kaspersky-Datenbanken und Programm-Module auf autonomen Geräten:

1. Verbinden Sie einen Wechseldatenträger mit dem Gerät, auf dem der Administrationsserver installiert ist.

2. Kopieren Sie die Update-Dateien auf den Wechseldatenträger.

   Standardmäßig befinden sich die Updates unter: \\<Servername>\KLSHARE\Updates.

   Alternativ können Sie Kaspersky Security Center so konfigurieren, dass es die Updates regelmäßig in einen von Ihnen gewählten Ordner kopiert. Verwenden Sie dazu die Option **Heruntergeladene Updates in zusätzliche Ordner kopieren** in den Eigenschaften der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*. Wenn Sie einen Ordner auf einem USB-Stick oder einer externen Festplatte als Zielordner für diese Option angeben, wird dieses Massenspeichergerät stets über die aktuellsten Versionen der Updates verfügen.

3. Konfigurieren Sie Kaspersky Endpoint Security für Linux auf autonomen Geräten so, dass Updates aus einem lokalen Ordner oder von einer freigegebenen Ressource (FTP-Server oder freigegebener Ordner) heruntergeladen werden.

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 Linux 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.

Verteilungspunkte und Verbindungs-Gateways anpassen

Die Struktur der Administrationsgruppen in Kaspersky Security Center Linux erfüllt folgende Funktionen:

- Gültigkeitsbereich der Richtlinien festlegen

  Mithilfe von *Richtlinienprofilen* existiert eine alternative Möglichkeit, um die notwendigen Einstellungen auf den Geräten anzuwenden.

- Gültigkeitsbereich der Gruppenaufgaben festlegen

  Es gibt eine Methode zur Festlegung des Gültigkeitsbereichs der Gruppenaufgaben, die nicht auf der Hierarchie der Administrationsgruppen basiert: die Nutzung von Aufgaben für die Geräteauswahlen und eine Reihe von Geräten.

- Festlegung der Zugriffsrechte auf die Geräte, sowie auf die virtuellen und sekundären Administrationsserver

- Verteilungspunkte zuweisen

Beim Aufbau der Struktur der Administrationsgruppen muss für eine optimale Bestimmung der Verteilungspunkte die Netzwerktopologie des Unternehmens berücksichtigt werden. Die optimale Zuordnung der Verteilungspunkte ermöglicht eine Verringerung des Netzwerkverkehrs innerhalb des Unternehmensnetzwerks.

Abhängig von der planmäßigen Struktur des Unternehmens und der Topologie der Netzwerke können die folgenden typischen Konfigurationen für die Struktur der Administrationsgruppen unterschieden werden:

- Einzelbüro
- Mehrere kleine, eigenständige Büros

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

Typische Konfiguration von Verteilungspunkten: Einzelbüro

In einer typischen Einzelbüro-Konfiguration befinden sich alle Geräte im Netzwerk des Unternehmens und können einander "sehen". Das Netzwerk des Unternehmens kann aus mehreren ausgewählten Teilen (der Netzwerke oder der Netzwerksegmente) bestehen, die über enge Kanäle verbunden sind.

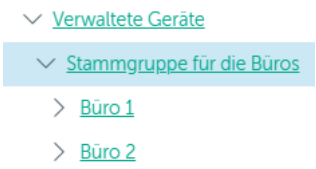
Es sind die folgenden Methoden für den Aufbau der Struktur der Administrationsgruppen möglich:

- Aufbau der Struktur der Administrationsgruppen unter Berücksichtigung der Netztopologie. Die Struktur der Administrationsgruppen muss die Netztopologie nicht unbedingt genau widerspiegeln. Es ist ausreichend, wenn den einzelnen Teilen des Netzwerkes bestimmte Administrationsgruppen entsprechen. Die Verteilungspunkte können automatisch bestimmt oder manuell zugewiesen werden.
- Aufbau der Struktur der Administrationsgruppen, in der die Netztopologie nicht widergespiegelt wird. In diesem Fall müssen Sie die automatische Bestimmung der Verteilungspunkte deaktivieren und dann für die Stammadministrationsgruppe in jedem ausgewählten Teil des Netzwerkes ein oder mehrere Geräte als Verteilungspunkte bestimmen, beispielsweise für die Gruppe **Verwaltete Geräte**. Alle Verteilungspunkte befinden sich dann auf einer Ebene und haben den identischen Gültigkeitsbereich, der alle Geräte im Netzwerk des Unternehmens umfasst. Jeder Administrationsagent wird in diesem Fall mit dem Verteilungspunkt verbunden, zu dem die Route am kürzesten ist. Die Route zum Verteilungspunkt kann mithilfe des Tools "tracert" bestimmt werden.

Typische Konfiguration von Verteilungspunkten: Mehrere kleine, eigenständige Büros

Diese typische Konfiguration entspricht einer Menge kleiner Remote-Büros, die eventuell durch das Internet mit dem Hauptbüro verbunden sind. Jedes der Remote-Büros befindet sich hinter einer NAT, das heißt ein Remote-Büro kann nicht mit einem anderen verbunden werden, die Büros sind voneinander isoliert.

Diese Konfiguration muss unbedingt in der Struktur der Administrationsgruppen widergespiegelt werden: für jedes Remote-Büros muss eine separate Administrationsgruppe erstellt werden (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 ausreichend freien Speicherplatz 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.

Berechnung der Anzahl und Konfiguration der Verteilungspunkte

Je mehr Client-Geräte ein Netzwerk enthält, desto mehr Verteilungspunkte sind erforderlich. Es wird empfohlen, die automatische Zuweisung von Verteilungspunkten nicht zu deaktivieren. Bei aktivierter automatischer Zuweisung der Verteilungspunkte weist der Administrationsserver bei einer großen Anzahl an Client-Geräten automatisch Verteilungspunkte zu und bestimmt ihre Konfiguration.

Verwendung exklusiv zugewiesener Verteilungspunkte

Wenn Sie planen, als Verteilungspunkte eine Reihe von bestimmten Geräten zu verwenden (d. h., exklusiv zugewiesene Server), so können Sie auf die automatische Zuweisung der Verteilungspunkte verzichten. Überzeugen Sie sich in diesem Fall davon, dass die Geräte, die Sie zu Verteilungspunkten bestimmen möchten, über ausreichend freien Speicherplatz auf dem Datenträger verfügen, nicht regelmäßig abgeschaltet werden und dass auf ihnen der Ruhezustand deaktiviert ist.

Anzahl der exklusiv zugewiesenen Verteilungspunkte in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, ein einzelnes Netzwerksegment enthält

Anzahl der Client-Geräte in dem Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 300	0 (Es müssen keine Verteilungspunkte bestimmt werden)
Über 300	Akzeptabel: (N/10.000 +1), empfohlen: (N/5000+2), wobei N die Anzahl an Geräten im Netzwerk ist

Anzahl der exklusiv zugewiesenen Verteilungspunkte in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, mehrere Netzwerksegmente enthält

Anzahl der Client-Geräte pro Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 10	0 (Es müssen keine Verteilungspunkte bestimmt werden)
10-100	1
Über 100	Akzeptabel: (N/10.000 +1), empfohlen: (N/5000+2), wobei N die Anzahl an Geräten im Netzwerk ist

Verwendung von Standard-Client-Geräten (Workstations) als Verteilungspunkte

Wenn Sie planen, als Verteilungspunkte Standard-Client-Geräte (d. h., Workstations) zu verwenden, wird zur Vermeidung einer unnötigen Belastung des Administrationsservers empfohlen, die Verteilungspunkte auf folgende Weise zuzuweisen (s. nachfolgende Tabelle):

Anzahl der als Verteilungspunkte fungierenden Workstations in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, ein einzelnes Netzwerksegment enthält

Anzahl der Client-Geräte in dem Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 300	0 (Es müssen keine Verteilungspunkte bestimmt werden)
Über 300	(N/300 +1), wobei N die Anzahl an Geräten im Netzwerk ist, jedoch mindestens 3 Verteilungspunkte

Anzahl der als Verteilungspunkte fungierenden Workstations in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, mehrere Netzwerksegmente enthält

Anzahl der Client-Geräte pro Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 10	0 (Es müssen keine Verteilungspunkte bestimmt werden)
10-30	1
31-300	2
Über 300	(N/300 +1), wobei N die Anzahl an Geräten im Netzwerk ist, jedoch mindestens 3 Verteilungspunkte

Wenn ein Verteilungspunkt abgeschaltet (oder aus anderen Gründen nicht verfügbar) ist, können die verwalteten Geräte in seinem Bereich Updates vom Administrationsserver abrufen.

Verteilungspunkte automatisch zuweisen

Es wird empfohlen, die Verteilungspunkte automatisch zu bestimmen. In diesem Fall wählt Kaspersky Security Center Linux die Geräte, die zu Verteilungspunkten bestimmt werden, selbständig aus.

Um Verteilungspunkte automatisch zuzuweisen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptfenster der Anwendung neben dem Namen des benötigten Administrationsservers auf das Symbol **Einstellungen** ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

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

3. Wählen Sie die Option **Verteilungspunkte automatisch zuweisen** aus.

   Wenn die automatische Bestimmung der Verteilungspunkte aktiviert ist, können die Einstellungen der Verteilungspunkte nicht manuell angepasst werden und die Liste der Verteilungspunkte kann nicht verändert werden.

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

Daraufhin beginnt der Administrationsserver damit, Verteilungspunkte automatisch zu bestimmen und ihre Einstellungen zu konfigurieren.

Verteilungspunkte manuell zuweisen

In Kaspersky Security Center Linux haben Sie die Möglichkeit, Geräte manuell zu Verteilungspunkten zu bestimmen.

Es wird empfohlen, die Verteilungspunkte automatisch zu bestimmen. In diesem Fall wählt Kaspersky Security Center Linux die Geräte, die zu Verteilungspunkten bestimmt werden, selbständig aus. Wenn Sie jedoch aus bestimmten Gründen auf die automatische Bestimmung der Verteilungspunkte verzichten möchten (beispielsweise wenn Sie speziell ausgewählte Server verwenden wollen), können Sie die Verteilungspunkte manuell bestimmen, nachdem Sie deren Anzahl und Konfiguration berechnet haben.

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

Um ein Gerät manuell zum Verteilungspunkt zu bestimmen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptfenster der Anwendung neben dem Namen des benötigten Administrationsservers auf das Symbol **Einstellungen** ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

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

3. Wählen Sie die Option **Verteilungspunkte manuell zuweisen** aus.

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

5. Wählen Sie das Gerät aus, das Sie zu einem Verteilungspunkt machen möchten.

   Berücksichtigen Sie bei der Auswahl des Geräts die Besonderheiten des Verteilungspunkts und die Anforderungen an das Gerät, das die Rolle des Verteilungspunkts übernehmen soll.

6. Wählen Sie die Administrationsgruppe aus, die zum Gültigkeitsbereich des ausgewählten Verteilungspunkts gehören soll.

7. Klicken Sie auf die Schaltfläche **Uhrzeit der Verschlüsselung**.

   Der hinzugefügte Verteilungspunkt wird in der Liste der Verteilungspunkte im Abschnitt **Verteilungspunkte** angezeigt.

8. Wählen Sie den hinzugefügten Verteilungspunkt in der Liste aus und öffnen Sie sein Eigenschaftenfenster.

9. 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-Portnummer**

       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 Linux automatisch eine eindeutige IP-Multicast-Adresse innerhalb des angegeben Bereichs 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.

- Geben Sie im Abschnitt **Bereich** die Administrationsgruppen an, an die der Verteilungspunkt Updates verteilen soll.
- Im Abschnitt **Update-Quelle** können Sie eine Update-Quelle für den Verteilungspunkt auswählen:
  - **Update-Quelle**

    Wählen Sie eine Update-Quelle für den Verteilungspunkt aus:
    - Damit der Verteilungspunkt die Updates vom Administrationsserver erhält, wählen Sie **Vom Administrationsserver beziehen**.
    - Damit Verteilungspunkte Updates anhand einer Aufgabe beziehen können, wählen Sie **Aufgaben zum Update-Download verwenden** aus und geben Sie anschließend eine Aufgabe vom Typ *Download von Updates in die Datenverwaltung der Verteilungspunkte* an:
      - Wenn eine solche Aufgabe bereits auf dem Gerät vorhanden ist, wählen Sie die Aufgabe in der Liste aus.
      - Wenn auf dem Gerät noch keine derartige Aufgabe vorhanden ist, klicken Sie auf den Link **Aufgabe erstellen**, um eine Aufgabe zu erstellen. Der Assistent zum Hinzufügen von Aufgaben wird gestartet. Folgen Sie den Anweisungen des Assistenten.
  - **Diff-Dateien herunterladen**

    Diese Option aktiviert die Funktion zum Download von Diff-Dateien.

    Diese Option ist standardmäßig aktiviert.
- Konfigurieren Sie die Abfrage von IP-Bereichen durch den Verteilungspunkt.
  - **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 **Abfragen mit Zeroconf-Technologie aktivieren** 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.
- Geben Sie im Abschnitt **Erweitert** den Ordner an, den der Verteilungspunkt zum Speichern der zu verteilenden Daten verwenden soll.
  - **Standardordner verwenden**

    Bei Auswahl dieser Option wird zum Speichern der Ordner auf dem Verteilungspunkt verwendet, in dem der Administrationsagent installiert wurde.
  - **Benutzerdefinierten Ordner verwenden**

Bei Auswahl dieser Option können Sie im unteren Feld den Pfad zum Ordner angeben. Dabei können Sie einen lokalen Ordner des Verteilungspunkts oder einen Ordner auf einem beliebigen, sich im Unternehmensnetzwerk befindlichen Remote-Gerät angeben.

Das Benutzerkonto, unter dem der Administrationsagent auf dem Verteilungspunkt gestartet wird, muss über die Lese- und Schreibberechtigungen für den angegebenen Ordner verfügen.

10. Klicken Sie auf die Schaltfläche **Uhrzeit der Verschlüsselung**.

Daraufhin übernehmen die ausgewählten Geräte die Rolle des Verteilungspunkts.

Liste mit Verteilungspunkten für eine Administrationsgruppe bearbeiten

Sie können eine Liste mit Verteilungspunkten anzeigen, die einer bestimmten Administrationsgruppe zugewiesen wurden, und Verteilungspunkte zu dieser Liste hinzufügen oder daraus löschen.

Um die Liste mit Verteilungspunkten, die einer Administrationsgruppe zugewiesen wurden, zu bearbeiten, gehen Sie wie folgt vor:

1. Gehen Sie 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.

Einen Push-Server aktivieren

In Kaspersky Security Center kann ein Verteilungspunkt als Push-Server für Geräte fungieren, die über das mobile Protokoll oder über den Administrationsagenten verwaltet werden. Ein Push-Server muss beispielsweise aktiviert sein, wenn Sie die erzwungene Synchronisierung von KasperskyOS-Geräten mit dem Administrationsserver verwenden möchten. Ein Push-Server besitzt denselben Umfang verwalteter Geräte wie der Verteilungspunkt, auf dem der Push-Server aktiviert ist. Wenn Sie mehrere Verteilungspunkte derselben Administrationsgruppe zugewiesen haben, können Sie den Push-Server auf jedem der Verteilungspunkte aktivieren. In diesem Fall verteilt der Administrationsserver die Last zwischen den Verteilungspunkten.

Möglicherweise möchten Sie Verteilungspunkte als Push-Server verwenden, um sicherzustellen, dass eine kontinuierliche Verbindung zwischen einem verwalteten Gerät und dem Administrationsserver besteht. Für einige Vorgänge ist eine durchgängige Verbindung erforderlich, z. B. das Starten und Stoppen lokaler Aufgaben, das Empfangen von Statistiken für ein verwaltetes Programm oder die Herstellung eines Tunnels. Wenn Sie einen Verteilungspunkt als Push-Server verwenden, müssen Sie weder die Option **Verbindung zum Administrationsserver nicht trennen** auf verwalteten Geräten verwenden, noch Pakete an den UDP-Port des Administrationsagenten senden.

Ein Push-Server unterstützt die Last von bis zu 50.000 gleichzeitigen Verbindungen.

So aktivieren Sie Push-Server auf einem Verteilungspunkt:

1. Klicken Sie auf das Symbol **Einstellungen** ( ) neben dem Namen des benötigten Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

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

3. Klicken Sie auf den Namen des Verteilungspunkts, auf dem Sie den Push-Server aktivieren möchten.

   Das Eigenschaftenfenster des Verteilungspunkts wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Allgemein** die Option **Push-Server ausführen**.

5. Geben Sie im Feld **Push-Server-Port** die Portnummer ein. Sie können die Nummer eines beliebigen unbelegten Ports angeben.

6. Geben Sie im Feld **Remote-Host-Adresse** die IP-Adresse oder den Namen des Geräts mit dem Verteilungspunkt an.

7. Klicken Sie auf die Schaltfläche **Uhrzeit der Verschlüsselung**.

Der Push-Server ist auf dem ausgewählten Verteilungspunkt aktiviert.

Verwalten von Programmen von Drittanbietern auf Client-Geräten

In diesem Abschnitt werden die Funktionen von Kaspersky Security Center Linux für die Verwaltung von Drittanbieter-Programmen beschrieben, die auf Client-Geräten ausgeführt werden.

Szenario: Programmverwaltung

Sie können den Start von Programmen auf Benutzergeräten verwalten. Sie können zulassen oder blockieren, dass Programme auf verwalteten Geräten ausgeführt werden. Verwenden Sie dazu die Komponente "Programmkontrolle".

Die Komponente "Programmkontrolle" ist für Kaspersky Endpoint Security 11.2 für Linux und neuere Versionen verfügbar.

Erforderliche Maßnahmen

- Kaspersky Security Center Linux ist in Ihrem Unternehmen bereitgestellt.
- Die Richtlinie "Kaspersky Endpoint Security für Linux" wurde erstellt und ist aktiv.

Schritte

Die Nutzung der Programmkontrolle erfolgt schrittweise:

1. **Erstellen und Anzeigen der Liste der ausführbaren Dateien auf Client-Geräten**

   Dieser Schritt unterstützt Sie dabei, herauszufinden, welche ausführbaren Dateien sich auf verwalteten Geräten befinden. Öffnen Sie die Liste der ausführbaren Dateien und vergleichen Sie sie 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.

   Anleitungen: Liste der auf Client-Geräten gespeicherten ausführbaren Dateien abrufen und anzeigen

2. **Erstellen von Programmkategorien für die im Unternehmen verwendeten Programme**

   Analysieren Sie die Listen der 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.

   Anleitungen: Erstellen einer manuell zu erweiternden Programmkategorie

3. **Konfigurieren der "Programmkontrolle" in der Richtlinie von Kaspersky Endpoint Security für Linux**

   Konfigurieren Sie die Komponente "Programmkontrolle" in der Richtlinie von Kaspersky Endpoint Security für Linux anhand der Programmkategorien, die Sie beim vorherigen Schritt erstellt haben.

4. **Überprüfen der Konfiguration der Programmkontrolle**

   Stellen Sie sicher, dass folgende Aktionen ausgeführt wurden:

- Erstellen von Programmkategorien
- Konfigurieren der Programmkontrolle mit den Programmkategorien

Ergebnisse

Wenn das Szenario abgeschlossen ist, wird der Start von Programmen auf verwalteten Geräten gesteuert. Die Benutzer können nur jene Programme starten, die in Ihrem Unternehmen erlaubt sind. Im Unternehmen verbotene Programme können nicht gestartet werden.

Ausführliche Informationen zur "Programmkontrolle" finden Sie in der Online-Hilfe zu 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 für Kaspersky Endpoint Security 11.2 für Linux und neuere Versionen verfügbar.

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. Dieser Modus 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 Linux können Sie nur Kategorien mit manuell hinzugefügten Inhalten erstellen. Sie definieren Bedingungen, z. B. Dateimetadaten, Datei-Hashcode, Dateizertifikat, KL-Kategorie oder Dateipfad, um ausführbare Dateien in die Kategorie aufzunehmen.

Ausführliche Informationen zur "Programmkontrolle" finden Sie in der Online-Hilfe zu Kaspersky Endpoint Security für Linux.

Abrufen und Anzeigen einer Liste der auf Client-Geräten gespeicherten ausführbaren Dateien

Sie können eine Liste der auf verwalteten Geräten gespeicherten ausführbaren Dateien abrufen. Um ausführbare Dateien zu inventarisieren, müssen Sie eine Inventarisierungsaufgabe erstellen.

Die Funktion zur Inventarisierung ausführbarer Dateien ist für Kaspersky Endpoint Security 11.2 für Linux und neuere Versionen verfügbar.

Um eine Inventarisierungsaufgabe für ausführbare Dateien auf den Client-Geräten zu erstellen, gehen Sie folgendermaßen vor:

1. Gehen Sie 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** die Option "Kaspersky Endpoint Security für Linux" aus.

4. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Inventarisierung** aus.

5. Klicken Sie auf der Seite **Erstellung der Aufgabe abschließen** auf **Fertigstellen**.

   Nach Abschluss des Assistenten für das Erstellen einer Aufgabe wird die Aufgabe **Inventarisierung** erstellt und angepasst. Wenn Sie möchten, können Sie die Einstellungen für die erstellte Aufgabe ändern. Daraufhin wird die neu erstellte Aufgabe in der Aufgabenliste angezeigt.

Eine ausführliche Beschreibung der Inventarisierungsaufgabe finden Sie in der Online-Hilfe zu Kaspersky Endpoint Security für Linux.

Nach Ausführung der Aufgabe **Inventarisierung** wird die Liste der auf verwalteten Geräten gespeicherten ausführbaren Dateien erstellt und Sie können die Liste anzeigen.

Während der Inventarisierung werden ausführbare Dateien folgender Formate erkannt: mz, com, pe, ne, sys, cmd, bat, ps1, js, vbs, reg, msi, cpl, dll, jar, sowie HTML-Dateien.

Um sich die Liste aller auf den Client-Geräten gespeicherten ausführbaren Dateien anzeigen zu lassen, gehen Sie wie folgt vor:

Wählen Sie in der Dropdown-Liste unter **VORGÄNGE → DRITTANBIETER-PROGRAMME** den Punkt **AUSFÜHRBARE DATEIEN** aus.

Auf der Seite wird die Liste der auf Client-Geräten gespeicherten ausführbaren Dateien angezeigt.

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. Wählen Sie in der Dropdown-Liste unter **VORGÄNGE → DRITTANBIETER-PROGRAMME** den Punkt **PROGRAMMKATEGORIEN** aus.

   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. Klicken Sie auf der Seite **Bedingungen** des Assistenten auf **Hinzufügen**, um ein Bedingungskriterium für das Aufnehmen von Dateien in die Kategorie hinzuzufügen.

5. Wählen Sie auf der Seite **Bedingungskriterien** einen Regeltyp zum Erstellen einer Kategorie aus der Liste aus:

   - 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 Linux 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 für Linux unterstützen die SHA-256-Berechnung.

  Wählen Sie eine der Optionen zur Berechnung der Hash-Funktion für die Dateien der Kategorie durch Kaspersky Security Center Linux aus:

  - Wenn alle in Ihrem Netzwerk installierten Instanzen von Sicherheits-Apps das Programm Kaspersky Endpoint Security für Linux darstellen, aktivieren Sie das Kontrollkästchen **Fehleranzahl**.

  - Aktivieren Sie das Kontrollkästchen **MD5-Hash** nur dann, wenn Sie Kaspersky Endpoint Security für Windows verwenden. Die MD5-Hash-Funktion wird von Kaspersky Endpoint Security für Linux nicht unterstützt.

  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 archiviertem Ordner

Wenn diese Option ausgewählt ist, können Sie eine Datei eines archivierten Ordners angeben und dann auswählen, welche Bedingung Sie verwenden möchten, um Programme zu der Benutzerkategorie hinzuzufügen. Der archivierte Ordner wird entpackt und die von Ihnen ausgewählten Bedingungen werden auf die Dateien in diesem Ordner angewendet. Sie können eine der folgenden Kriterien als Bedingung auswählen:

- **Dateihash**

  Sie wählen aus, mit welcher Hash-Funktion (MD5 oder SHA-256) die Hash-Werte berechnet werden sollen. Programme, die denselben Hash-Wert haben wie die Dateien in dem archivierten Ordner, werden in die benutzerdefinierte Programmkategorie aufgenommen.

  Wählen Sie nur dann eine MD5-Hash-Funktion aus, wenn Sie Kaspersky Endpoint Security für Windows verwenden. Die MD5-Hash-Funktion wird von Kaspersky Endpoint Security für Linux nicht unterstützt.

- **Metadaten**

  Sie wählen aus, welche Metadaten Sie als Kriterien verwenden möchten. Ausführbare Dateien mit denselben Metadaten werden in die benutzerdefinierte Programmkategorie aufgenommen.

- **Zertifikat**

  Sie wählen aus, welche Zertifikatseigenschaften (Zertifikatssubjekt, Fingerabdruck oder Aussteller) Sie als Kriterien verwenden möchten. Ausführbare Dateien, die mit dem Zertifikat signiert sind, das identische Eigenschaften hat, werden zur Benutzerkategorie hinzugefügt.

Das ausgewählte Kriterium wird zur Liste mit Kriterien hinzugefügt.

Sie können so viele Kriterien in die erstellende Programmkategorie aufnehmen, wie Sie benötigen.

6. Klicken Sie auf der Seite **Ausschlüsse** des Assistenten auf **Hinzufügen**, um ein exklusives Bedingungskriterium hinzufügen, nach dem Dateien aus der gerade erstellten Kategorie ausgeschlossen werden sollen.

7. Wählen Sie auf der Seite **Bedingungskriterien** einen Regeltyp aus der Liste aus, so wie Sie einen Regeltyp zum Erstellen einer Kategorie ausgewählt haben.

Wenn der Assistent beendet ist, 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 der Online-Hilfe zu Kaspersky Endpoint Security für Linux.

Liste der Programmkategorien anzeigen

Sie können die Liste der angepassten Programmkategorien und die Einstellungen der einzelnen Programmkategorien anzeigen.

Um die Liste der Programmkategorien anzuzeigen,

Wählen Sie auf der Registerkarte **VORGÄNGE** in der Dropdown-Liste **DRITTANBIETER-PROGRAMME** den Abschnitt **PROGRAMMKATEGORIEN** aus.

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.

Ereignisbezogene ausführbare Dateien zur Programmkategorie hinzufügen

Nachdem Sie die "Programmkontrolle" in den Richtlinien von Kaspersky Endpoint Security für Linux 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. Gehen Sie 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)**

  Wählen Sie diese Option nur aus, wenn Sie Kaspersky Endpoint Security für Windows verwenden. Eine MD5-Hash-Funktion wird von Kaspersky Endpoint Security für Linux nicht unterstützt.

  Jede Datei hat ihre eindeutige Hash-Funktion MD5. Bei der Auswahl der Hash-Funktion MD5 enthält die Kategorie nur die entsprechende Datei, beispielsweise die angegebene Programmversion.

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

   Nach Abschluss des Assistenten werden ausführbare Dateien, die sich auf Programmkontrollereignisse 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 der Online-Hilfe zu Kaspersky Endpoint Security für Linux.

Überwachung und Berichterstattung

In diesem Abschnitt werden die Möglichkeiten für die Überwachung und die Berichterstellung von Kaspersky Security Center Linux beschrieben. Diese Möglichkeiten geben Ihnen einen Überblick über Ihre Infrastruktur, die Schutzstatus und Statistiken.

Nach der Bereitstellung von Kaspersky Security Center Linux oder während des Programmbetriebs können Sie die Funktionen für die Überwachung und für die Berichterstellung an Ihre Bedürfnisse anpassen.

Szenario: Überwachung und Berichterstattung

Dieser Abschnitt enthält ein Szenario zur Konfiguration der Funktion der Überwachung und Berichterstellung in Kaspersky Security Center Linux.

Erforderliche Komponenten

Nach der Verteilung von Kaspersky Security Center Linux im Unternehmensnetzwerk können Sie mit seiner Überwachung beginnen und Berichte zum Netzwerkbetrieb erstellen.

Die Überwachung und Berichterstellung in einem Unternehmensnetzwerk erfolgt in mehreren Etappen:

1. **Einstellungen zum Umschalten der Status von Geräten**

   Machen Sie sich mit den Einstellungen des von bestimmten Bedingungen abhängigen Gerätestatus vertraut. Wenn Sie diese Einstellungen anpassen, können Sie auch die Anzahl der Ereignisse der Ereigniskategorie *Kritisch* oder *Warnung* ändern. Beachten Sie bei der Konfiguration des Wechsels des Gerätestatus Folgendes:

   - Die neuen Einstellungen widersprechen nicht den Richtlinien zur Informationssicherheit Ihres Unternehmens.
   - Sie können rechtzeitig auf wichtige Ereignisse der Informationssicherheit in Ihrem Unternehmensnetzwerk reagieren.

2. **Einstellungen für Benachrichtigungen über Ereignisse auf Client-Geräten anpassen**

   Anleitung:

   Passen Sie die Benachrichtigungen (per E-Mail, SMS oder durch Start einer ausführbaren Datei) zu Ereignissen auf Client-Geräten an

3. **Empfohlene Aktionen für kritische und warnende Benachrichtigungen ausführen**

   Anleitung:

   Führen Sie die empfohlenen Aktionen für Ihr Unternehmensnetzwerk aus

4. **Sicherheitsstatus Ihres Unternehmensnetzwerks verfolgen**

   Anleitung:

   - Sehen Sie sich das Widget Schutzstatus an
   - Erstellen und überprüfen Sie den Bericht über den Schutzstatus
   - Erstellen und überprüfen Sie den Fehlerbericht

5. **Client-Geräte finden, die nicht geschützt sind**

Anleitung:

- Sehen Sie sich das Widget Neue Geräte an
- Erstellen und überprüfen Sie den Bericht über die Bereitstellung des Schutzes

6. **Schutz der Client-Geräte überprüfen**

   Anleitung:

   - Erstellen und lesen Sie Berichte der Kategorien Schutzstatus und Bedrohungsstatistiken
   - Starten Sie überprüfen Sie sie die Ereignisauswahl mit dem Wert "Kritisch"

7. **Ereignismenge für Datenbank einschätzen und einschränken**

   Informationen über Ereignisse im Betrieb 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:

   - Maximale Anzahl der Ereignisse einschränken

8. **Lizenzinformationen überprüfen**

   Anleitung:

   - Fügen Sie das Widget Nutzung von Lizenzschlüsseln zum Dashboard hinzu und sehen Sie es sich an
   - Erstellen und überprüfen Sie den Bericht über die Lizenzschlüsselnutzung

Ergebnisse

Nach Abschluss des Szenarios werden Sie über den Schutz Ihres Unternehmensnetzwerks informiert und können Aktionen für den weiteren Schutz des Netzwerks planen.

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 14 Web Console die folgenden Arten der Überwachung und Berichterstattung in Ihrem Unternehmensnetzwerk:

- Dashboard
- Berichte
- Ereignisauswahlen
- Benachrichtigungen

Dashboard

Das Dashboard bietet eine grafische Darstellung von Informationen und erlaubt Ihnen, sicherheitsrelevante Entwicklungen in Ihrem Unternehmensnetzwerk zu überwachen.

Berichte

Mithilfe von Berichten können Sie detaillierte, zahlenbasierte Informationen zur Sicherheit Ihres Unternehmensnetzwerkes zusammenstellen und diese Informationen in einer Datei speichern, per E-Mail versenden und ausdrucken.

Ereignisauswahlen

Die Ereignisauswahlen bieten eine Bildschirmansicht der benannten Ereignisgruppen, die aus der Administrationsserver-Datenbank ausgewählt wurden. Diese Sätze von Ereignissen sind nach den folgenden Kategorien gruppiert:

- Nach Ereigniskategorie – **Kritische Ereignisse**, **Funktionsfehler**, **Warnungen** und **Informative Ereignisse**
- Nach Zeit – **Letzte Ereignisse**
- Nach Typ – **Benutzeranfragen** und **Audit-Ereignisse**

Benutzerdefinierte Ereignisauswahlen können Sie auf der Basis von Einstellungen, die in der Oberfläche von Kaspersky Security Center 14 Web Console verfügbar sind, erstellen und anzeigen.

Benachrichtigungen

Benachrichtigungen informieren Sie über Ereignisse und unterstützen Sie dabei, mithilfe empfohlener Maßnahmen oder mit Maßnahmen, die Sie als geeignet erachten, schneller auf diese Ereignisse zu reagieren.

Dashboard und Widgets

Dieser Abschnitt enthält Informationen über das Dashboard und die Widgets, die vom Dashboard bereitgestellt werden. Der Abschnitt enthält Anweisungen zum Verwalten von Widgets und zum Konfigurieren von Widget-Einstellungen.

Dashboard verwenden

Das Dashboard bietet eine grafische Darstellung von Informationen und erlaubt Ihnen, sicherheitsrelevante Entwicklungen in Ihrem Unternehmensnetzwerk zu überwachen.

Das Dashboard finden Sie in der Kaspersky Security Center 14 Web Console im Abschnitt **ÜBERWACHUNG UND BERICHTERSTATTUNG** unter **DASHBOARD**.

Das Dashboard enthält Widgets, die angepasst werden können. Sie können aus einer großen Anzahl an unterschiedlichen Widgets auswählen, die als Kreis- oder Ringdiagramme, Tabellen, Grafiken, Balkendiagramme und Listen dargestellt werden. Die in den Widgets angezeigten Informationen werden automatisch aktualisiert und das Aktualisierungsintervall beträgt ein bis zwei Minuten. Das Aktualisierungsintervall unterscheidet sich von Widget zu Widget. Über das Einstellungsmenü können Sie die Daten eines Widgets jederzeit manuell aktualisieren.

Standardmäßig enthalten Widgets Informationen über alle Ereignisse, die in der Datenbank des Administrationsservers gespeichert sind.

Die Kaspersky Security Center 14 Web 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 Symbol **Einstellungen** (⚙) neben dem Widget, das Sie ausblenden möchten.
3. Wählen Sie **Web-Widget verbergen** aus.

4. Klicken Sie im folgenden Fenster **Warnung** auf **Uhrzeit der Verschlüsselung**.

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 Symbol **Einstellungen** (⚙) 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 Symbol **Einstellungen** (⚙) 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 Symbol **Einstellungen** (⚙) 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 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 im Abschnitt **BENUTZER UND ROLLEN → BENUTZER** 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**.
2. Klicken Sie auf den Namen des Benutzerkontos, für welches Sie das Dashboard mit Widgets anpassen möchten.
3. Öffnen Sie im folgenden Fenster mit den Kontoeinstellungen die Registerkarte **Dashboard**.

   Auf der sich öffnenden Registerkarte wird Ihnen das gleiche Dashboard angezeigt wie dem Benutzer.
4. Wenn die Option **Konsole im Nur-Dashboard-Modus anzeigen** aktiviert ist, klicken Sie auf den Umschalter, um sie zu deaktivieren.

   Wenn diese Option aktiviert ist, können auch Sie das Dashboard nicht ändern. Nachdem Sie die Option deaktiviert haben, können Sie Widgets verwalten.
5. Konfigurieren Sie das Erscheinungsbild des Dashboards. Der auf der Registerkarte **Dashboard** angezeigte Satz von Widgets steht dem Benutzer mit dem anpassbaren Konto zur Verfügung. Er oder sie kann weder die Einstellungen noch die Größe der Widgets ändern, und keine Widgets zum Dashboard hinzufügen oder daraus entfernen. Daher müssen Sie für den Benutzer die Widgets anpassen, damit er oder sie die Statistiken zum Netzwerkschutz anzeigen kann. Um dies zu tun, können Sie auf der Registerkarte **Dashboard** die gleichen Vorgänge mit den Widgets ausführen, wie im Abschnitt **ÜBERWACHUNG UND BERICHTERSTATTUNG → DASHBOARD**:
   - Dem Dashboard neue Widgets hinzufügen.
   - Vom Nutzer nicht benötigte Widgets ausblenden.
   - Widgets verschieben, sodass sie einer bestimmten Reihenfolge entsprechen.
   - Die Größe oder das Aussehen von Widgets ändern.
   - Die Einstellungen von Widgets ändern.
6. Klicken Sie auf den Umschalter, um die Option **Konsole im Nur-Dashboard-Modus anzeigen** zu aktivieren.

Anschließend steht dem Benutzer nur noch das Dashboard zur Verfügung. Er oder sie kann Statistiken überwachen, aber die Schutzeinstellungen des Netzwerks und das Erscheinungsbild des Dashboards nicht ändern. Da für Sie das gleiche Dashboard wie für den Benutzer angezeigt wird, können auch Sie das Dashboard nicht ändern.

Wenn Sie die Option deaktiviert lassen, wird dem Benutzer das Hauptmenü angezeigt, sodass er verschiedene Aktionen in Kaspersky Security Center ausführen kann, einschließlich der Änderung von Sicherheitseinstellungen und Widgets.

7. Wenn Sie die Konfiguration des Nur-Dashboard-Modus abgeschlossen haben, klicken Sie auf **Speichern**. Erst im Anschluss wird dem Benutzer das konfigurierte Dashboard angezeigt.

8. Wenn der Benutzer zum Anzeigen der Statistiken von unterstützten Kaspersky-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 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 14 Web Console in dem Abschnitt **ÜBERWACHUNG UND BERICHTERSTATTUNG** unter **BERICHTE**.

Standardmäßig enthalten Berichte Informationen für die letzten 30 Tage.

Kaspersky Security Center Linux besitzt eine Standardauswahl an Berichten für die 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** 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** 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 **Uhrzeit der Verschlüsselung**, 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.

       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 Standard wird Port 1000 verwendet.

     - **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 Standard wird Port 1 verwendet. Sie sollten diesen Wert ändern, wenn Sie Informationen von sekundären Administrationsservern sammeln müssen, die sich auf niedrigeren Ebenen in der Struktur befinden.

- **Auf Daten warten (Min.)**

  Vor Erstellen des Berichts wartet der Administrationsserver, für den die Berichtsvorlage erstellt wurde, während der angegebenen Anzahl von Minuten auf Daten von sekundären Administrationsservern. Wenn nach Ablauf dieses Zeitraums keine Daten von einem sekundären Administrationsserver eingehen, wird der Bericht dennoch ausgeführt. Anstelle der eigentlichen Daten zeigt der Bericht Daten aus dem Cache (wenn die Option **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 Standard wird Port 0 verwendet.

- **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. Klicken Sie auf die Schaltfläche **Schließen** (⨯), um das Fenster **Bearbeiten des Berichts <Berichtsname>** zu schließen.

Der aktualisierte Bericht wird in der Liste der Berichtsvorlagen angezeigt.

Exportieren eines Berichts in eine Datei

Sie können einen Bericht in eine XML- oder HTML-Datei exportieren.

So exportieren Sie einen Bericht in eine Datei:

1. Gehen Sie zu **ÜBERWACHUNG UND BERICHTERSTATTUNG → BERICHTE**.
2. Aktivieren Sie das Kontrollkästchen neben dem Bericht, den Sie in eine Datei exportieren möchten.
3. Klicken Sie auf die Schaltfläche **Bericht exportieren**.
4. Ändern Sie im folgenden Fenster den Namen der Berichtsdatei im Feld **Das APNs-Zertifikat läuft bald ab**. Standardmäßig stimmt der Dateiname mit dem Namen der ausgewählten Berichtsvorlage überein.
5. Wählen Sie den Berichtsdateityp aus: XML, HTML oder PDF.

Um einen Bericht ins PDF-Format zu konvertieren, wird das Tool wkhtmltopdf benötigt. Wenn Sie die Option PDF auswählen, überprüft der Administrationsserver, ob das Tool wkhtmltopdf auf dem Gerät installiert ist. Ist das Tool nicht installiert, meldet das Programm, dass dieses Tool auf dem Administrationsserver-Gerät installiert werden muss. Installieren Sie das Tool manuell und gehen Sie dann zum nächsten Schritt.

6. Klicken Sie auf die Schaltfläche **Bericht exportieren**.

   Der Bericht im ausgewählten Format wird in den Standardordner Ihres Geräts heruntergeladen, oder es öffnet sich ein Standard-**Speichern unter**-Fenster in Ihrem Browser, in dem Sie die Datei an der gewünschten Stelle speichern können.

Der Bericht wird in die Datei gespeichert.

Bericht erstellen und anzeigen

Um einen Bericht zu erstellen und anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **ÜBERWACHUNG UND BERICHTERSTATTUNG → BERICHTE**.
2. Klicken Sie auf den Namen der Berichtsvorlage, die Sie zum Erstellen eines Berichts verwenden möchten.

Ein Bericht, der die ausgewählte Vorlage verwendet, wird erstellt angezeigt.

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 **Abbrechen der Operation ist nicht erlaubt** 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. Gehen Sie 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.

      Um einen Bericht ins PDF-Format zu konvertieren, wird das Tool wkhtmltopdf benötigt. Wenn Sie die Option PDF auswählen, überprüft der Administrationsserver, ob das Tool wkhtmltopdf auf dem Gerät installiert ist. Ist das Tool nicht installiert, meldet das Programm, dass dieses Tool auf dem Administrationsserver-Gerät installiert werden muss. Installieren Sie das Tool manuell und gehen Sie dann zum nächsten Schritt.

   c. Ob die Berichte per E-Mail gesendet werden sollen; welche Einstellungen für die Benachrichtigung per E-Mail verwendet werden sollen.

   d. Ob die Berichte in einem Ordner gespeichert werden sollen; ob zuvor gespeicherte Berichte in diesem Ordner überschrieben werden sollen; ob ein bestimmtes Benutzerkonto für den Zugriff auf den Ordner verwendet werden soll (bei freigegebenen Ordnern).

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 **Uhrzeit der Verschlüsselung**, 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 Linux auftretenden Ereignistypen, und zur Verwaltung der Blockierung häufiger Ereignisse.

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 14 Web Console verfügbar sind, erstellen und anzeigen.

Ereignisauswahlen finden Sie in Kaspersky Security Center 14 Web Console im Abschnitt **ÜBERWACHUNG UND BERICHTERSTATTUNG** unter **EREIGNISAUSWAHLEN**.

Standardmäßig enthalten Ereignisauswahlen Informationen für die letzten sieben Tage.

Kaspersky Security Center Linux besitzt eine Standardauswahl von (vordefinierten) Ereignisauswahlen:

- Ereignisse mit unterschiedlichen Ereigniskategorien:
  - **Kritische Ereignisse**
  - **Funktionsfehler**
  - **Warnungen**
  - **Informative Ereignisse**
- **Benutzeranfragen** (Ereignisse der verwalteten Programme)
- **Letzte Ereignisse** (der letzten Woche)
- Audit-Ereignisse

Sie können auch zusätzliche benutzerdefinierte Auswahlen definieren und anpassen. In benutzerdefinierten Auswahlen können Sie Ereignisse nach den Eigenschaften der Geräte, von denen sie stammen, (Gerätenamen, IP-Bereiche und Administrationsgruppen), nach Ereignistypen und Signifikanz, 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 Linux 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.

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.

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 **Uhrzeit der Verschlüsselung**.

   Die Ereignisauswahl ist gelöscht.

Speicherdauer für ein Ereignis festlegen

Kaspersky Security Center Linux 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. Möglicherweise sollen bestimmte Ereignisse länger oder kürzer aufbewahrt werden, als durch die Standardwerte festgelegt. Sie können die Standardeinstellungen der Speicherdauer für ein Ereignis ändern.

Wenn Sie bestimmte Ereignisse nicht in der Administrationsserver-Datenbank speichern möchten, können Sie die entsprechende Einstellung deaktivieren. Verwenden Sie dazu die Administrationsserver-Richtlinie und die Richtlinie der Kaspersky-Anwendung oder die Administrationsserver-Eigenschaften (nur für Administrationsserver-Ereignisse). Dadurch wird die Anzahl der Ereignistypen in der Datenbank reduziert.

Je länger die Speicherdauer eines Ereignisses, desto schneller erreicht die Datenbank ihre maximale Kapazität. Eine längere Speicherdauer für ein Ereignis ermöglicht es Ihnen aber, Überwachungs- und Berichtsaufgaben über einen längeren Zeitraum durchzuführen.

So legen Sie die Speicherdauer für ein Ereignis in der Datenbank des Administrationsservers fest:

1. Wählen Sie **GERÄTE → RICHTLINIEN UND PROFILE** aus.
2. Führen Sie eine der folgenden Aktionen aus:

   - Um die Speicherdauer für die Ereignisse des Administrationsagenten oder eines verwalteten Kaspersky-Programms anzupassen, klicken Sie auf den Namen der entsprechenden Richtlinie.

     Die Eigenschaftenseite der Richtlinie wird geöffnet.

   - Um die Administrationsserver-Ereignisse anzupassen, klicken Sie im oberen Bereich des Bildschirms auf das Symbol **Einstellungen** () neben dem Namen des entsprechenden Administrationsservers.

     Wenn Sie eine Richtlinie für den Administrationsserver haben, können Sie stattdessen auf den Namen dieser Richtlinie klicken.

Die Eigenschaftenseite des Administrationsservers (oder die Eigenschaftenseite der Administrationsserver-Richtlinie) wird geöffnet.

3. Wählen Sie die Registerkarte **Konfiguration von Ereignissen** aus.

   Eine Liste der Ereignistypen, die sich auf den Abschnitt **Kritisch** beziehen, wird angezeigt.

4. Wählen Sie **Funktionsfehler**, **Warnung** oder **Information** aus.

5. Klicken Sie in der Liste der Ereignistypen im rechten Bereich auf den Link für das Ereignis, dessen Speicherdauer Sie ändern möchten.

   Im Abschnitt **Ereignisregistrierung** des sich öffnenden Fensters ist die Option **In der Administrationsserver-Datenbank speichern für (Tage)** aktiviert.

6. Geben Sie im Bearbeitungsfeld unterhalb dieser Umschalttaste die Anzahl der Tage ein, über die das Ereignis gespeichert werden soll.

7. Wenn Sie ein Ereignis nicht in der Administrationsserver-Datenbank speichern möchten, deaktivieren Sie die Option **In der Administrationsserver-Datenbank speichern für (Tage)**.

   Wenn Sie Administrationsserver-Ereignisse im Eigenschaftenfenster des Administrationsservers anpassen und wenn die Ereigniseinstellungen in der Richtlinie des Kaspersky Security Center Linux Administrationsservers gesperrt sind, können Sie die Speicherdauer für ein Ereignis nicht ändern.

8. Klicken Sie auf die Schaltfläche **Uhrzeit der Verschlüsselung**.

   Das Eigenschaftenfenster der Richtlinie wird geschlossen.

Die Ereignisse des ausgewählten Typs, die vom Administrationsserver empfangen und gespeichert werden, besitzen ab jetzt die geänderte Speicherfrist. Für zuvor empfangene Ereignisse ändert der Administrationsserver die Speicherfrist nicht.

Ereignistypen

Jede Komponente von Kaspersky Security Center Linux hat einen eigenen Satz von Ereignistypen. Dieser Abschnitt enthält eine Liste mit Ereignissen, die auf dem Administrationsserver von Kaspersky Security Center Linux und im Administrationsagenten auftreten können. Die Typen der Ereignisse, die in den Programmen von Kaspersky auftreten, sind in diesem Abschnitt nicht aufgeführt.

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 Linux angezeigt, wenn Sie Ereignisse konfigurieren und wenn diese auftreten.
- **Ereignistyp-ID**. Dieser numerische Code wird verwendet, wenn Sie Ereignisse zwecks Ereignisanalyse mithilfe von Drittanbieter-Tools verarbeiten.
- **Ereignistyp** (alphabetischer Code). Dieser Code wird verwendet, wenn Sie Ereignisse mithilfe der in der Datenbank von Kaspersky Security Center Linux verfügbaren öffentlichen Ansichten durchsuchen und

verarbeiten und wenn Ereignisse in ein SIEM-System exportiert werden.

- **Beschreibung**. Dieser Text beschreibt die Situationen, in denen ein Ereignis eintreffen kann, und gibt Hinweise auf weiteres Vorgehen.

- **Standard-Speicherdauer**. Das ist die Anzahl der Tage, die ein Ereignis in der 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. Wenn Sie angegeben haben, dass solche Ereignisse im Ereignisprotokoll des Betriebssystems gespeichert werden sollen, finden Sie die Ereignisse hier.

  Sie können die Speicherdauer für Ereignisse ändern: Legen Sie die Speicherdauer für ein Ereignis fest.

Ereignisse des Administrationsservers

Dieser Abschnitt informiert über die Ereignisse, die sich auf den Administrationsserver beziehen.

Ereignisse des Administrationsservers: Kritisch

Die folgende Tabelle enthält die Ereignisse des Kaspersky Security Center Linux Administrationsservers mit der Ereigniskategorie **Kritisch**.

Ereignisse des Administrationsservers: Kritisch

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung
Lizenzbeschränkung wurde überschritten	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Kaspersky Security Center Linux überprüft einmal täglich, ob 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 Lizenzeinheiten die von einer Lizenz abgedeckten werden, 110% der von der Lizenz abgedeckten Gesamtzahl an Einheiten überschreitet.

			Auch wenn dieses Ereignis eintritt, werden die Client-Geräte geschützt. Sie können auf dieses Ereignis folgendermaßen reagieren: • Schauen Sie sich die Liste der verwalteten Geräte an. Löschen Sie ungenutzte Geräte. • Stellen Sie eine Lizenz für weitere Geräte zur Verfügung (fügen Sie dem Administrationsserver einen gültigen Aktivierungscode oder eine Schlüsseldatei hinzu). Kaspersky Security Center Linux ermittelt die Regeln zum Auslösen von Ereignissen, wenn eine Lizenzbeschränkung überschritten wurde.
Das Gerät wird nicht mehr verwaltet	4111	KLSRV_HOST_OUT_CONTROL	Ereignisse dieser Art treten auf, wenn ein verwaltetes Gerät ist im Netzwerk sichtbar ist, es aber über einen bestimmten Zeitraum keine Verbindung zum Administrationsserver hergestellt hat. Finden Sie heraus, warum der Administrationsagent auf diesem Gerät nicht ordnungsgemäß ausgeführt wird. Mögliche Ursachen können Netzwerkprobleme oder das Entfernen des Administrationsagenten von diesem Gerät sein.
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.
Die Schlüsseldatei wurde der Deny-Liste hinzugefügt	4124	KLSRV_LICENSE_BLACKLISTED	Ereignisse dieser Art treten auf, wenn Kaspersky den von Ihnen verwendeten Aktivierungscode oder die Schlüsseldatei auf die Deny-Liste setzt. Kontaktieren Sie den Technischen Support für weitere Informationen.
Die Lizenz läuft bald ab	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Ereignisse dieser Art treten auf, wenn das Ablaufdatum einer kommerziellen Lizenz näher rückt. Einmal am Tag überprüft Kaspersky Security Center, ob sich das Ablaufdatum der Lizenz nähert. Veröffentlicht werden Ereignisse dieses Typs 30 Tage, 15 Tage, 5 Tage und 1 Tag vor dem Ablaufdatum der Lizenz. Die Anzahl der Tage kann nicht geändert werden. Wird der Administrationsserver an dem entsprechenden Tag vor dem Ablaufdatum der Lizenz deaktiviert, so wird das Ereignis erst am darauf folgenden Tag veröffentlicht. Wenn die kommerzielle Lizenz abläuft, stellt Kaspersky Security Center Lizenz nur grundlegende Funktionen bereit. Sie können auf dieses Ereignis folgendermaßen reagieren: • Vergewissern Sie sich, dass dem Administrationsserver ein Reserve-Lizenzschlüssel hinzugefügt wurde. • Wenn Sie ein Abonnement verwenden, stellen

			Sie sicher, dies zu Verlängern. Ein unbeschränktes Abonnement wird automatisch verlängert, falls der vereinbarte Betrag bis zum Fälligkeitsdatum an den Dienstleister überwiesen wird.
Das Zertifikat ist abgelaufen	4132	KLSRV_CERTIFICATE_EXPIRED	Ereignisse dieser Art treten auf, wenn das Administrationsserver-Zertifikat für die Funktion "Mobile Geräte verwalten" abläuft. Sie müssen das abgelaufene Zertifikat aktualisieren. Sie können die automatische Aktualisierung des Zertifikats konfigurieren, indem Sie das Kontrollkästchen **Zertifikat automatisch neu veröffentlichen, falls möglich** in den Einstellungen der Zertifikatsausstellung aktivieren.

Ereignisse des Administrationsservers: Funktionsfehler

Die folgende Tabelle enthält die Ereignisse des Kaspersky Security Center Linux Administrationsservers mit der Ereigniskategorie **Funktionsfehler**.

Ereignisse des Administrationsservers: Funktionsfehler

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung
Laufzeitfehler	4125	KLSRV_RUNTIME_ERROR	Ereignisse dieser Art tret bei unbekannten Problem auf. Dabei handelt es sich meistens um DBMS-Probleme, Netzwerkprob und andere Hard- und Softwareprobleme. Informationen zu diesem Ereignis stehen in der Ereignisbeschreibung.

Für eine der lizenzierten Programmgruppen wurde die Beschränkung für die Anzahl von Installationen überschritten	4126	KLSRV_INVLICPROD_EXCEDED	Der Administrationsserve generiert Ereignisse dies Art periodisch (stündlich Ereignisse dieser Art tret auf, wenn Sie in Kaspersk Security Center Linux die Lizenzschlüssel von Drittanbieter-Programme verwalten und wenn die Anzahl der Installationen Limit überschreitet, das durch den Lizenzschlüsse des Drittanbieter-Progra festgelegt ist. Sie können auf dieses Ereignis folgendermaßen reagieren: • Schauen Sie sich die L der verwalteten Gerä an. Löschen Sie Drittanbieter-Progran von den Geräten, auf denen sie nicht verwe werden. • Verwenden Sie eine Drittanbieter-Lizenz f mehr Geräte. Sie können die Lizenzschlüssel von Drittanbieter-Programme verwalten, indem Sie die Funktionen der lizenziert Programmgruppe verwer Zur lizenzierten Programmgruppe gehöre Drittanbieter-Programme welche die von Ihnen festgelegten Kriterien erfüllen.
Kopieren der Updates in den angegebenen Ordner nicht ausgeführt	4123	KLSRV_UPD_REPL_FAIL	Ereignisse dieser Art tret auf, wenn Software-Upda in einen oder mehrere zusätzlich freigegebene Ordner kopiert werden. Sie können auf dieses Ereignis folgendermaßen reagieren: • Prüfen Sie, ob das Benutzerkonto, das fü den Zugriff auf die Or verwendet wird, über Berechtigung zum Schreiben verfügt.

			• Prüfen Sie, ob sich de Benutzername und/o das Kennwort für den oder die Ordner geän haben. • Überprüfen Sie die Internetverbindung, d die Ursache des Ereignisses sein kann. Folgen Sie den Anweisungen, um die Datenbanken und die Programm-Module zu aktualisieren.
Kein freier Platz auf dem Datenträger	4107	KLSRV_DISK_FULL	Ereignisse dieser Art tret auf, wenn auf der Festpla des Geräts, auf dem der Administrationsserver installiert ist, freier Speicherplatz knapp wird Schaffen Sie freien Speicherplatz.
Kein Zugriff auf freigegebenen Ordner	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Ereignisse dieser Art tret auf, wenn der Freigegebe Ordner des Administrationsservers n verfügbar ist. Sie können auf dieses Ereignis folgendermaßen reagieren: • Überprüfen Sie, ob de Administrationsserve (auf dem sich der freigegebene Ordner befindet) angeschalte und erreichbar ist. • Prüfen Sie, ob sich de Benutzername und/o das Kennwort zu dies Ordner geändert hab • Prüfen Sie die Netzwerkverbindung.
Die Administrationsserver-Datenbank ist nicht verfügbar	4109	KLSRV_DATABASE_UNAVAILABLE	Ereignisse dieser Art tret auf, wenn der Administrationsserver nic verfügbar ist. Sie können auf dieses Ereignis folgendermaßen reagieren:

			• Prüfen Sie, ob der Remote-Server, auf d SQL Server installiert verfügbar ist. • Schauen Sie in die Protokolle des DBMS, die Ursache für die Nichtverfügbarkeit de Datenbank des Administrationsserve finden. Beispielsweise kann aufgrund von präventiven Wartungsarbeiten de Remote-Server, auf d SQL Server installiert nicht verfügbar sein.
Kein freier Platz in der Administrationsserver-Datenbank	4110	KLSRV_DATABASE_FULL	Ereignisse dieser Art tret auf, wenn in der Datenba des Administrationsserve kein freier Speicherplatz mehr vorhanden ist. Der Administrationsserve funktioniert nicht, wenn s Datenbank die Kapazitätsgrenze erreich und wenn weiteres Speic in der Datenbank nicht möglich ist. Im Folgenden die Gründe dieses Ereignis, in Abhängigkeit zu dem DBI dass Sie verwenden, sow geeignete Reaktionen au dieses Ereignis: • Wenn Sie als DBMS d SQL Server Express Edition verwenden: • Konsultieren Sie di Dokumentation vo SQL Server Expre Edition und sucher nach der Größenbeschränk der von Ihnen genutzten Version Wahrscheinlich ha Datenbank Ihres Administrationsse die Größenbeschränk der Datenbank überschritten.

			• Begrenzung der A der Ereignisse, die der Datenbank des Administrationsse gespeichert werde sollen. • In der Datenbank d Administrationsse befinden sich zu vi Ereignisse, die dur die Komponente "Programmkontrol gesendet wurden. können die Einstellungen der Richtlinie in Kasper Endpoint Security Linux, die sich auf Speicherung von Ereignissen der Programmkontrolle der Datenbank des Administrationsse bezieht, ändern. • Wenn Sie ein anderes DBMS als SQL Server Express Edition verwenden: • Begrenzen Sie nich die Anzahl der Ereignisse, die in d Datenbank des Administrationsse gespeichert werde sollen. • Verringern Sie die an Ereignissen, die der Datenbank des Administrationsse gespeichert werde sollen. Überprüfen Sie die Informationen zur Auswa des DBMS.

Ereignisse des Administrationsservers: Warnung

Die folgende Tabelle enthält die Ereignisse des Kaspersky Security Center Linux Administrationsservers mit der Ereigniskategorie **Warnung**.

Ereignisse des Administrationsservers: Warnung

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung
Lizenzbeschränkung wurde überschritten	4098	KLSRV_EV_LICENSE_CHECK_100_110	Kaspersky Security Center Linux überprüf einmal täglich, ob eine Lizenzbeschränkung überschritten wurde. Ereignisse dieser Art treten auf, wenn der Administrationsserver erkennt, dass Beschränkungen der Lizenz durch Kaspersk Anwendungen, die auf den Client-Geräten installiert sind, überschritten werden. Außerdem tritt das Ereignis auf, wenn die Anzahl der aktuell genutzten Lizenzeinhe die von einer Lizenz abgedeckten werden, 100% bis 110% der von Lizenz abgedeckten Gesamtzahl an Einheit überschreitet. Auch wenn dieses Ere eintritt, werden die Cli Geräte geschützt. Sie können auf dieses Ereignis folgendermaß reagieren: • Schauen Sie sich d Liste der verwaltet Geräte an. Löscher Sie ungenutzte Geräte. • Stellen Sie eine Liz für weitere Geräte Verfügung (fügen S dem Administrationsser einen gültigen Aktivierungscode o eine Schlüsseldate hinzu). Kaspersky Security Center Linux ermittelt Regeln zum Auslösen v Ereignissen, wenn eine Lizenzbeschränkung überschritten wurde.
Das Gerät war lange Zeit im Netzwerk	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Ereignisse dieser Art treten auf, wenn ein

inaktiv			verwaltetes Gerät für längere Zeit inaktiv erscheint. Dies ist meistens dann Fall, wenn ein verwalte Gerät ausrangiert wur Sie können auf dieses Ereignis folgendermaß reagieren: • Löschen Sie das G manuell aus der Lis der verwalteten Geräte. Geben Sie mithilfe Kaspersky Security Center 14 Web Console den Zeitra an, nach dessen Ablauf das Ereignis **Das Gerät war lan Zeit im Netzwerk inaktiv** erstellt wird • Geben Sie mithilfe Kaspersky Security Center 14 Web Console den Zeitra an, nach dessen Ablauf das Gerät automatisch aus de Gruppe entfernt w
Konflikt von Gerätenamen	4102	KLSRV_EVENT_HOSTS_CONFLICT	Ereignisse dieser Art treten auf, wenn der Administrationsserver zwei oder mehr verwal Geräte als ein Gerät wahrnimmt. Dies ist meistens dann Fall, wenn ein geklonte Laufwerk für die Softwareverteilung au verwalteten Geräten verwendet wurde, und dabei der Administrationsagent einem Referenzgerät r in den Modus für dezidierte Laufwerke geschaltet wurde.

			Um diesen Fehler zu vermeiden, schalten S den Administrationsagente auf einem Referenzge in den Modus zum Klor von Laufwerken, bevo das Laufwerk dieses Gerätes klonen.
Gerätestatus - "Warnung"	4114	KLSRV_HOST_STATUS_WARNING	Ereignisse dieser Art treten auf, wenn einen verwalteten Gerät der Status *Warnung* zugewiesen wird. Sie können die Bedingung anpassen, unter dener der Gerätestatus zu *Warnung* wechselt.
Für eine der lizenzierten Programmgruppen wird die Beschränkung für die Anzahl von Installationen bald überschritten	4127	KLSRV_INVLICPROD_FILLED	Ereignisse dieser Art treten auf, wenn die Anzahl der Installation von Drittherstellter-Programmen, die in eir lizenzierten Programmgruppe enthalten sein dürfen, 90% des in den Eigenschaften des Lizenzschlüssels angegeben zulässigen Werts erreicht. Sie können auf dieses Ereignis folgendermaß reagieren: • Wenn das Drittherstellter-Programm auf einig verwalteten Geräte nicht verwendet wi löschen Sie das Programm von dies Geräten. • Wenn Sie erwarten dass die Anzahl der Installationen des Drittherstellter-Programms das Maximum in nächst Zukunft übersteigt sollten Sie im Vorfe den Erwerb einer Drittherstellter-Lize für eine größere Anzahl an Geräten Erwägung ziehen.

			Sie können die Lizenzschlüssel von Drittanbieter-Programmen verwalte indem Sie die Funktior der lizenzierten Programmgruppe verwenden.
Zertifikat wurde angefordert	4133	KLSRV_CERTIFICATE_REQUESTED	Ereignisse dieser Art treten auf, wenn das automatische Neuausstellen eines Zertifikats für die Funktion "Mobile Gerä verwalten" fehlschlägt Im Folgenden werden Ursachen für das Ereig und angebrachte Reaktionen darauf ausgeführt: • Die automatische Neuausstellung wu für ein Zertifikat initiiert, für das die Option **Zertifikat automatisch neu veröffentlichen, fa möglich** deaktivier Dies kann aufgrunc eines Fehler geschehen, der bei Erstellung des Zertifikats auftrat. manuelles Neuausstellen des Zertifikats kann notwendig sein. • Wenn Sie eine Integration mit eine Public-Key-Infrastruktur verwenden, kann ei fehlendes Namensattribut de SAM-Benutzerkon welches für die PKI Integration und zur Ausstellen der Zertifikate genutzt wird, die Ursache s Überprüfen Sie die Eigenschaften des Benutzerkontos.
Zertifikat wurde entfernt	4134	KLSRV_CERTIFICATE_REMOVED	Ereignisse dieser Art treten auf, wenn ein

			Administrator ein Zertifikat beliebiger Ar (General, Mail, VPN) fü die Funktion "Mobile Geräte verwalten" entfernt. Nach dem Entfernen eines Zertifikats schläg für die mobilen Geräte über dieses Zertifikat verbunden sind, die Verbindung mit dem Administrationsserver fehl. Dieses Ereignis kann hilfreich sein, wenn es darum geht, Fehlfunktionen im Zusammenhang mit de Verwaltung mobiler Geräte aufzuspüren.
Das APNs-Zertifikat ist abgelaufen	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Ereignisse dieser Art treten auf, wenn ein APNs-Zertifikat abläuf Sie müssen manuell da APNs-Zertifikat erneu und es auf einem iOS MDM-Server installiere
Das APNs-Zertifikat läuft bald ab	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Ereignisse dieser Art treten auf, wenn das APNs-Zertifikat in wer als 14 Tagen abläuft. Wenn das APNs-Zerti abläuft, müssen Sie manuell das APNs-Zertifikat erneuern und auf einem iOS MDM-Server installieren. Es wird empfohlen, das Sie den Zeitpunkt für d Erneuern des APNs-Zertifikats vor das Ablaufdatum legen.
Die FCM-Nachricht konnten nicht an das mobile Gerät gesendet werden	4138	KLSRV_GCM_DEVICE_ERROR	Ereignisse dieser Art treten auf, wenn die Funktion "Mobile Gerä verwalten" so konfigur ist, dass sie Google Firebase Cloud Messa (FCM) für die Verbindu verwalteter Geräte mi Android-Betriebssyste verwendet, und auf de FCM-Server das Bearbeiten von empfangenen

			Administrationsserver Anfragen fehlschlägt. bedeutet, dass einige verwalteten mobilen Geräte keine PUSH-Benachrichtigungen empfangen. Studieren Sie den HTT Code in den Details de Ereignisbeschreibung reagieren Sie entsprechend. Weiter Informationen über HT Codes, die vom FCM-Server empfangen wurden, und damit verbundene Fehler, entnehmen Sie bitte d Dokumentation von Google Firebase Servi (siehe Kapitel "Antwortcodes für nachgeschaltete Nachrichtenfehler").
HTTP-Fehler beim Versenden der FCM-Nachricht an den FCM-Server	4139	KLSRV_GCM_HTTP_ERROR	Ereignisse dieser Art treten auf, wenn die Funktion "Mobile Gerä verwalten" so konfigur ist, dass sie Google Firebase Cloud Messa (FCM) für die Verbindu verwalteter Geräte mi Android-Betriebssyste verwendet, und der FC Server auf eine Administrationsserver Anfrage einen anderer HTTP-Code als 200 (" zurück zurückgibt. Im Folgenden werden Ursachen für das Ereig und angebrachte Reaktionen darauf ausgeführt: • Probleme mit dem FCM-Server. Studieren Sie den HTTP-Code in den Details der Ereignisbeschreibu und reagieren Sie entsprechend. Wei Informationen über HTTP-Codes, die v FCM-Server empfangen wurder und damit verbund Fehler, entnehmen

			bitte der Dokumentation vo Google Firebase Service (siehe Kapi "Antwortcodes für nachgeschaltete Nachrichtenfehler" • Probleme mit dem Proxyserver (wenn einen Proxyserver benutzen). Studier Sie den HTTP-Cod den Details des Ereignisses und reagieren Sie entsprechend.
Die FCM-Nachricht konnte nicht an den FCM-Server gesendet werden	4140	KLSRV_GCM_GENERAL_ERROR	Ereignisse diese Art treten auf, wenn im Rahmen der Verwendu des Google Firebase Cloud Messaging HTT Protokolls unerwartete Fehler auf dem Administrationsserver auftreten. Studieren Sie die Informationen in der Ereignisbeschreibung reagieren Sie entsprechend. Wenn Sie selbst keine Lösung für dieses Problem ausmachen können, ist es empfehlenswert den Technischen Support Kaspersky zu kontaktieren.
Auf der Festplatte ist wenig freier Platz vorhanden	4105	KLSRV_NO_SPACE_ON_VOLUMES	Ereignisse dieser Art treten auf, wenn auf d Gerät, auf dem der Administrationsserver installiert ist, der Speicherplatz knapp w Schaffen Sie freien Speicherplatz.
Wenig freier Platz in der Administrationsserver-Datenbank	4106	KLSRV_NO_SPACE_IN_DATABASE	Ereignisse dieser Art treten auf, wenn der P in der Datenbank des Administrationsserver knapp ist. Wenn Sie di Situation nicht lösen, erreicht die Datenbanl des

				Administrationsserver bald ihre Kapazitätsgre und der Administrationsserver wird nicht länger funktionieren. Nachfolgend finden Si die Ursachen für diese Ereignis in Abhängigke vom DBMS, das Sie verwenden, sowie geeignete Reaktionen dieses Ereignis. Wenn Sie als DBMS di SQL Server Express Edition verwenden: • Konsultieren Sie die Dokumentation vo SQL Server Expres Edition und suchen nach der Größenbeschränku der von Ihnen genutzten Version. Wahrscheinlich wir die Datenbank Ihres Administrationsser die Größenbeschränku der Datenbank bald erreichen. • Begrenzung der An der Ereignisse, die i der Datenbank des Administrationsser gespeichert werde sollen. • In der Datenbank d Administrationsser befinden sich zu vie Ereignisse, die durc die Komponente "Programmkontrolle gesendet wurden. S können die Einstellungen der Richtlinie in Kasper Endpoint Security Linux, die sich auf d Speicherung von Ereignissen der Programmkontrolle der Datenbank des Administrationsser bezieht, ändern.

			Wenn Sie ein ander DBMS als SQL Ser Express Edition verwenden: • Begrenzen Sie nich die Anzahl der Ereignisse, die in de Datenbank des Administrationsser gespeichert werde sollen. • Reduzieren Sie die Liste an Ereignisse die in der Datenbar des Administrationsser gespeichert werde sollen. Überprüfen Sie die Informationen zur Aus des DBMS.
Die Verbindung mit dem sekundären Administrationsserver wurde getrennt	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Ereignisse dieser Art treten auf, wenn die Verbindung zum sekundären Administrationsserver unterbrochen ist. Konsultieren Sie das Ereignisprotokoll "Kaspersky" des Gerät auf dem der sekundär Administrationsserver installiert ist, und reagieren Sie entsprechend.
Die Verbindung mit dem primären Administrationsserver wurde getrennt	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Ereignisse dieser Art treten auf, wenn die Verbindung zum primä Administrationsserver unterbrochen ist. Konsultieren Sie das Ereignisprotokoll "Kaspersky" des Gerät auf dem der primäre Administrationsserver installiert ist, und reagieren Sie entsprechend.
Neue Updates der Programm-Module von Kaspersky sind registriert	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Ereignisse dieser Art treten auf, wenn der Administrationsserver Kaspersky-Software, auf verwalteten Gerät installiert ist, neue

			Updates registriert, welche eine Genehmig für die Installation benötigen. Genehmigen Sie über Kaspersky Security Center Web Console Updates oder lehnen S die Updates ab.
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 Ereign aus der Datenbank des Administrationsserver begonnen hat, nachde die Kapazitätsgrenze d Datenbank des Administrationsserver erreicht wurde. Sie können auf dieses Ereignis folgendermaß reagieren: • Ändern Sie die maximale Anzahl vo Ereignissen, die in d Datenbank des Administrationsser gespeichert sind. • Reduzieren Sie die Liste an Ereignisse die in der Datenbar des Administrationsser gespeichert werde 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 Administrationsserver gelöscht wurden, nachdem die Kapazitätsgrenze der Datenbank des Administrationsserver erreicht wurde. Sie können auf dieses Ereignis folgendermaß reagieren: • Ändern Sie die zulässige maximale Anzahl von Ereignissen, die in d Datenbank des

			Administrationsser gespeichert sind. • Reduzieren Sie die Liste an Ereignisse die in der Datenbar des Administrationsser gespeichert werde sollen.

Ereignisse des Administrationsservers: Information

Die folgende Tabelle enthält die Ereignisse des Kaspersky Security Center Linux Administrationsservers mit der Ereigniskategorie **Information**.

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
Gerät wurde automatisch zur Gruppe hinzugefügt	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 überschritten (mehr als 95% verbraucht)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 Tage
Es wurden Dateien gefunden, die zur Analyse an Kaspersky gesendet werden	4131	KLSRV_APS_FILE_APPEARED	30 Tage
Die ID der FCM Instance hat sich auf diesem mobilen Gerät geändert	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 Tage
Updates wurden erfolgreich in den angegebenen Ordner kopiert	4122	KLSRV_UPD_REPL_OK	30 Tage
Die Verbindung mit dem sekundären Administrationsserver wurde hergestellt	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 Tage

Die Verbindung mit dem primären Administrationsserver wurde hergestellt	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 Tage
Datenbanken wurden aktualisiert	4144	KLSRV_UPD_BASES_UPDATED	30 Tage
Audit: Verbindung mit dem Administrationsserver wurde hergestellt	4147	KLAUD_EV_SERVERCONNECT	30 Tage
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 Verbindung mit dem Administrationsserver wurde unterbrochen	4151	KLAUD_EV_SERVERDISCONNECT	30 Tage
Audit: Objekteigenschaften wurden geändert	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 Tage
Audit: Benutzerrechte wurden geändert	4153	KLAUD_EV_OBJECTACLMODIFIED	30 Tage

Ereignisse des Administrationsagenten

Dieser Abschnitt informiert über die Ereignisse, die sich auf den Administrationsagenten beziehen.

Ereignisse des Administrationsagenten: Warnung

Die nachfolgende Tabelle enthält die Ereignisse des Kaspersky Security Center Administrationsagenten mit der Signifikanz **Warnung**.

Ereignisse des Administrationsagenten: Warnung

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer
Es ist ein Vorfall aufgetreten	549	GNRL_EV_APP_INCIDENT_OCCURED	30 Tage

Ereignisse des Administrationsagenten: Information

Die nachfolgende Tabelle enthält die Ereignisse des Kaspersky Security Center Administrationsagenten mit der Signifikanz **Information**.

Ereignisse des Administrationsagenten: Information

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer
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
Neues Gerät wurde hinzugefügt	7708	KLNAG_EV_DEVICE_ARRIVAL	30 Tage
Gerät wurde entfernt	7709	KLNAG_EV_DEVICE_REMOVE	30 Tage
Neues Gerät wurde erkannt	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 Tage
Gerät wurde autorisiert	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 Tage

Häufige auftretende Ereignisse blockieren

Dieser Abschnitt enthält Informationen zur Verwaltung des Blockierens häufig auftretender Ereignisse sowie zum Aufheben der Blockade häufig auftretender Ereignisse.

Über das Blockieren von häufig auftretenden Ereignissen

Ein verwaltetes Programm (z. B. Kaspersky Endpoint Security für Linux), das auf einem oder mehreren verwalteten Geräten installiert ist, sendet möglicherweise viele Ereignisse des gleichen Typs an den Administrationsserver. Das Empfangen häufig auftretender Ereignisse kann die Administrationsserver-Datenbank überlasten und führt zum Überschreiben anderer Ereignisse. Der Administrationsserver beginnt, die am häufigsten auftretenden Ereignisse zu blockieren, wenn die Anzahl aller empfangenen Ereignisse den für die Datenbank festgelegten Grenzwert überschreitet.

Der Administrationsserver blockiert den Empfang von häufig auftretenden Ereignissen automatisch. Sie können die häufig auftretenden Ereignisse nicht selbst blockieren und auch nicht festlegen, welche Ereignisse blockiert werden sollen.

Um herauszufinden, ob ein Ereignis blockiert wird, können Sie die Liste mit Benachrichtigung anzeigen oder überprüfen, ob das Ereignis im Abschnitt **Blockieren häufig auftretender Ereignisse** des Administrationsservers aufgeführt ist. Wenn das Ereignis blockiert ist, können Sie Folgendes tun:

- Wenn Sie verhindern möchten, dass die Datenbank überschrieben wird, können Sie das Empfangen dieser Ereignistypen weiterhin blockieren.
- Wenn Sie beispielsweise den Grund für das häufige Senden eines Ereignisses an den Administrationsserver ermitteln möchten, können Sie häufig auftretende Ereignisse entsperren und die Ereignisse dieses Typs auf diese Weise weiterhin empfangen.

- Wenn Sie die häufig auftretenden Ereignisse weiterhin so lange empfangen möchten, bis sie wieder blockiert werden, können Sie für die häufig auftretenden Ereignisse die Blockierung entfernen.

Das Blockieren von häufig auftretenden Ereignissen verwalten

Der Administrationsserver blockiert den automatischen Empfang von häufig auftretenden Ereignissen, aber Sie können die Blockade aufheben und häufig auftretende Ereignisse weiterhin empfangen. Sie können außerdem den Empfang häufig auftretender Ereignisse blockieren, deren Blockade Sie zuvor aufgehoben haben.

Um das Blockieren von häufig auftretenden Ereignissen zu verwalten:

1. Klicken Sie im Hauptfenster der Anwendung neben dem Namen des benötigten Administrationsservers auf das Symbol **Einstellungen** ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Blockieren häufig auftretender Ereignisse** aus.

3. Im Abschnitt **Blockieren häufig auftretender Ereignisse**:

   - Wenn Sie die Blockade des Empfangs häufig auftretender Ereignisse aufheben möchten:

     a. Wählen Sie die häufig auftretenden Ereignisse aus, die Sie entsperren möchten, und klicken Sie anschließend auf die Schaltfläche **Ausschließen**.

     b. Klicken Sie auf **Speichern**.

   - Um häufig auftretende Ereignisse zu blockieren:

     a. Wählen Sie die häufig auftretenden Ereignisse aus, die Sie blockieren möchten, und klicken Sie auf **Blockieren**.

     b. Klicken Sie auf **Speichern**.

Der Administrationsserver empfängt die entsperrten häufig auftretenden Ereignisse und empfängt keine blockierten häufig auftretende Ereignisse.

Die Blockade von häufig auftretenden Ereignissen aufheben

Sie können die Blockade für häufig auftretende Ereignisse aufheben und diese dadurch solange empfangen, bis der Administrationsserver diese häufig auftretenden Ereignissen erneut blockiert.

Um die Blockade für häufig auftretende Ereignisse aufzuheben:

1. Klicken Sie im Hauptfenster der Anwendung neben dem Namen des benötigten Administrationsservers auf das Symbol **Einstellungen** ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Blockieren häufig auftretender Ereignisse** aus.

3. Wählen Sie im Abschnitt **Blockieren häufig auftretender Ereignisse** die Arten häufig auftretender Ereignisse, für die Sie die Blockade aufheben möchten.

4. Klicken Sie auf **Blockade aufheben**.

Das häufig auftretende Ereignis wird aus der Liste der häufig auftretenden Ereignisse entfernt. Der Administrationsserver empfängt Ereignisse dieses Typs.

Ereignisse auf dem Administrationsserver verarbeiten und speichern

Die Informationen über die Ausführung des Programms und der verwalteten Geräte werden in der Datenbank des Administrationsservers gespeichert. Jedes Ereignis gehört einem bestimmten Typ und einer Ereigniskategorie (*Kritisches Ereignis*, *Funktionsfehler*, *Warnung*, *Infomeldung*) an. Abhängig von den Umständen, unter denen das Ereignis aufgetreten ist, können Ereignissen eines Typs vom Programm verschiedene Ereigniskategorien zugeordnet werden.

Die Typen und Ereigniskategorien können Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **Ereignisse konfigurieren** anzeigen. Ferner können Sie im Abschnitt **Ereignisse konfigurieren** die Einstellungen für die Verarbeitung der einzelnen Ereignisse durch den Administrationsserver anpassen:

- Ereignisse auf dem Administrationsserver und in den Ereignisprotokollen des Betriebssystems auf dem Gerät und auf dem Administrationsserver erfassen
- Benachrichtigungsmethode des Administrators über die Ereignisse (beispielsweise SMS, E-Mail-Nachricht)

Im Eigenschaftenfenster des Administrationsservers können Sie im Abschnitt **Ereignis-Datenverwaltung** die Einstellungen für das Speichern der Ereignisse in der Datenbank des Servers anpassen: Anzahl der Einträge über Ereignisse und Speicherdauer der Einträge beschränken. Wenn Sie die maximale Anzahl der Ereignisse angeben, berechnet die Anwendung einen ungefähren Wert des für die angegebene Zahl benötigten Speicherplatzes. Sie können diese ungefähre Berechnung verwenden, um zu überprüfen, ob Sie ausreichen freien Platz auf dem Laufwerk haben, um einen Überlauf der Datenbank zu vermeiden. Standardmäßig umfasst die Datenbank des Administrationsservers 400.000 Ereignisse. Die empfohlene Maximalgröße der Datenbank liegt bei 45 Millionen Ereignissen.

Wenn die Anzahl der Ereignisse in der Datenbank den vom Administrator angegebenen Maximalwert erreicht, werden die ältesten Ereignisse vom Programm gelöscht und durch neue überschrieben. Wenn der Administrationsserver alte Ereignisse löscht, kann er keine neuen Ereignisse in der Datenbank speichern. Während dieser Zeitspanne werden Informationen über abgelehnte Ereignisse in das Ereignisprotokoll "Kaspersky" geschrieben. Die neuen Ereignisse werden in die Warteschlange verschoben und dann in der Datenbank gespeichert, nachdem der Löschvorgang abgeschlossen wurde.

Benachrichtigungen und Gerätestatus

Dieser Abschnitt enthält Informationen zum Anzeigen von Benachrichtigungen, zum Konfigurieren der Zustellung von Benachrichtigungen, zum Verwenden des Gerätestatus und zum Aktivieren der Änderung von Statuswerten der Geräte.

Benachrichtigungen verwenden

Benachrichtigungen informieren Sie über Ereignisse und unterstützen Sie dabei, mithilfe empfohlener Maßnahmen oder mit Maßnahmen, die Sie als geeignet erachten, schneller auf diese Ereignisse zu reagieren.

Je nach ausgewählter Benachrichtigungsmethode, stehen die folgenden Benachrichtigungstypen zur Verfügung:

- Bildschirmbenachrichtigungen
- Benachrichtigungen per SMS
- Benachrichtigungen per E-Mail
- Benachrichtigungen per ausführbarer Datei oder Skript

Bildschirmbenachrichtigungen

Bildschirmbenachrichtigungen informieren Sie über Ereignisse, die in Ereigniskategorien gruppiert sind (*Kritisch*, *Warnung*, und *Information*).

Bildschirmbenachrichtigungen können zwei Status haben:

- *Geprüft*. Dies bedeutet, dass Sie die für diese Nachricht empfohlenen Maßnahmen durchgeführt haben oder dass Sie der Nachricht diesen Status manuell zugewiesen haben.
- *Ungeprüft*. Dies bedeutet, dass Sie die für diese Nachricht empfohlenen Maßnahmen nicht durchgeführt haben oder dass Sie der Nachricht diesen Status nicht manuell zugewiesen haben.

Standardmäßig enthält die Liste mit Benachrichtigungen die Nachrichten mit dem Status *Ungeprüft*.

Sie können Ihr Unternehmensnetzwerk durch das Anzeigen der Bildschirmbenachrichtigungen kontrollieren und in Echtzeit auf diese reagieren.

Benachrichtigungen per E-Mail, SMS und ausführbarer Datei oder Skript

Kaspersky Security Center Linux bietet die Möglichkeit, Ihr Unternehmensnetzwerk zu kontrollieren, indem Nachrichten über alle Ereignisse, die Sie als wichtig einstufen, versandt werden. Für jedes Ereignis können Sie Benachrichtigungen per E-Mail, per SMS oder durch das Starten einer ausführbaren Datei oder eines Skripts konfigurieren.

Nach dem Erhalten von Benachrichtigungen per E-Mail oder SMS können Sie entscheiden, wie Sie auf das Ereignis reagieren. Die Reaktion sollte diejenige sein, die für Ihr Unternehmensnetzwerk am geeignetsten ist. Durch den Start einer ausführbaren Datei oder eines Skripts, geben Sie eine vordefinierte Reaktion auf ein Ereignis an. Sie können den Start einer ausführbaren Datei oder eines Skripts auch als erste Reaktion auf ein Ereignis in Erwägung ziehen. Nachdem die ausführbare Datei gestartet wurde, können Sie weitere Schritte unternehmen, um auf das Ereignis zu reagieren.

Anzeigen von Bildschirmbenachrichtigungen

Es gibt drei Möglichkeiten, um Benachrichtigungen auf dem Bildschirm anzuzeigen:

- In dem Abschnitt **ÜBERWACHUNG UND BERICHTERSTATTUNG → BENACHRICHTIGUNGEN**. Hier können Sie Nachrichten über vordefinierte Kategorien anzeigen.
- In einem separaten Fenster, welches unabhängig davon, in welchem Abschnitt Sie sich gerade befinden, geöffnet werden kann. In diesem Fall können Sie Nachrichten als geprüft markieren.
- In dem Widget **Benachrichtigungen nach ausgewählter Signifikanz** im Abschnitt **ÜBERWACHUNG UND BERICHTERSTATTUNG → DASHBOARD**. In dem Widget können Sie nur Nachrichten der Ereigniskategorien *Kritisch* und *Warnung* ansehen.

Sie können Aktionen ausführen, z. B. als Reaktion auf ein Ereignis.

Um Benachrichtigungen vordefinierter Kategorien anzuzeigen:

1. Wechseln Sie im Hauptmenü zu **ÜBERWACHUNG UND BERICHTERSTATTUNG → BENACHRICHTIGUNGEN**.

   Im linken Bereich ist die Kategorie **Alle Benachrichtigungen** ausgewählt, und im rechten Bereich werden alle Nachrichten angezeigt.

2. Wählen Sie im linken Bereich eine der drei Kategorien:

   - **Softwareverteilung**
   - **Geräte**
   - **Schutz**
   - **Ende der Verwendungsdauer des Lizenzschlüssels am** (Diese Kategorie umfasst Benachrichtigungen über Programme von Kaspersky, die zum Download verfügbar sind und Benachrichtigungen über Updates der Antiviren-Datenbanken, die heruntergeladen wurden.)
   - **Exploit-Prävention**
   - **Administrationsserver** (Diese Kategorie umfasst Ereignisse, die nur den Administrationsserver betreffen.)
   - **Nützliche Links** (Diese Kategorie umfasst Links zu Ressourcen von Kaspersky, z. B. zum Technischen Support von Kaspersky, dem Forum von Kaspersky, der Seite für Lizenzverlängerung und der Kaspersky IT Enzyklopädie.)
   - **Neuigkeiten von Kaspersky** (Diese Kategorie enthält Informationen über Veröffentlichungen von Kaspersky-Programmen.)

   Eine Liste mit Nachrichten zu den ausgewählten Kategorien wird angezeigt. Die Liste enthält Folgendes:

- Symbol, das dem Thema der Benachrichtigung entspricht: Softwareverteilung (), Schutz (), Update (), Geräteverwaltung (), Exploit-Prävention (), Administrationsserver ().
- Ereigniskategorie der Nachricht. Angezeigt werden Nachrichten mit den folgenden Ereigniskategorien: **Kritische Benachrichtigungen** (), **Warnende Benachrichtigungen** (), **Informative Benachrichtigungen**. Die Benachrichtigungen in der Liste sind nach Ereigniskategorien gruppiert.
- **Benachrichtigung**. Dies beinhaltet eine Beschreibung der Nachricht.
- **Aktion**. Dies beinhaltet einen Link zu einer empfohlenen Sofortmaßnahme. Über diesen Link können Sie beispielsweise in die Datenverwaltung wechseln und Sicherheitsanwendungen auf Geräten installieren, oder sich eine Liste mit Geräten oder Ereignissen anzeigen lassen. Nachdem die empfohlene Maßnahme für die Nachricht durchgeführt wurde, wird der Nachricht der Status *Geprüft* zugewiesen.
- **Status registriert**. Dies beinhaltet die Anzahl der vergangenen Tage und Stunden, seit die Nachricht auf dem Administrationsserver registriert wurde.

Um Bildschirmbenachrichtigungen nach Ereigniskategorien in einem separaten Fenster anzuzeigen:

1. Klicken Sie in der rechten oberen Ecke der Kaspersky Security Center 14 Web Console auf das **Flaggen**-Symbol ().

Wenn das **Flaggensymbol** einen roten Punkt besitzt, existieren Nachrichten, die noch nicht geprüft wurden.

Es öffnet sich ein Fenster mit der Liste von Nachrichten. Standardmäßig ist die Registerkarte **Alle Benachrichtigungen** ausgewählt und die Nachrichten sind nach Ereigniskategorie gruppiert: *Kritisch*, *Warnung*, und *Information*.

2. Wählen Sie die Registerkarte **System** aus.

   Die Liste der Nachrichten mit den Ereigniskategorien *Kritisch* ( ) und *Warnung* ( ) wird angezeigt. Die Liste der Nachrichten enthält Folgendes:

   - Eine Farbmarkierung. Kritische Benachrichtigungen sind rot markiert. Warnende Benachrichtigungen sind gelb markiert.
   - Symbol, welches das Thema der Benachrichtigung angibt: Softwareverteilung ( ), Schutz ( ), Update ( ), Geräteverwaltung ( ), Exploit-Prävention ( ), Administrationsserver ( ).
   - Eine Beschreibung der Nachricht.
   - **Flaggensymbol**. Das **Flaggen**-Symbol ist grau, wenn Benachrichtigungen der Status *Ungeprüft* zugewiesen wurden. Wenn Sie das graue **Flaggen**-Symbol auswählen und einer Nachricht den Status *Geprüft* zuweisen, ändert sich die Farbe des Symbols zu weiß.
   - Link zur empfohlenen Maßnahme. Wenn Sie auf den Link klicken und anschließend die empfohlene Maßnahme durchführen, erhält die Nachricht den Status *Geprüft*.
   - Die Anzahl der vergangenen Tage seit die Nachricht auf dem Administrationsserver registriert wurde.

3. Wählen Sie die Registerkarte **Mehr** aus.

   Die Liste der Benachrichtigungen mit der Ereigniskategorie *Information* wird angezeigt.

   Der Aufbau der Liste ist identisch mit dem der Liste für die Registerkarte **System** (siehe oben). Der einzige Unterschied ist die fehlende Farbmarkierung.

Sie können Benachrichtigungen nach dem Datumsintervall, in welchem sie auf dem Administrationsserver registriert wurden, filtern. Benutzen Sie das Kontrollkästchen **Filter anzeigen** um den Filter zu verwalten.

Um Bildschirmbenachrichtigungen im Widget anzuzeigen:

1. Wählen Sie im Abschnitt **DASHBOARD** den Punkt **Web-Widget hinzufügen oder wiederherstellen**.
2. Klicken Sie in dem sich öffnenden Fenster auf die Kategorie **Andere**, wählen Sie das Widget **Benachrichtigungen nach ausgewählter Signifikanz** aus, und klicken Sie auf Hinzufügen.

   Das Widget erscheint jetzt auf der Registerkarte **DASHBOARD**. Standardmäßig zeigt das Widget Benachrichtigungen mit der Ereigniskategorie *Kritisch* an.

   Sie können in dem Widget auf die Schaltfläche **Einstellungen** klicken und die Einstellungen des Widgets ändern, um Nachrichten mit der Ereigniskategorie *Warnung* anzuzeigen. Oder Sie können mittels **Benachrichtigungen nach ausgewählter Signifikanz**, ein weiteres Widget mit der Ereigniskategorie *Warnung* hinzufügen.

   Die Liste der Benachrichtigungen ist im Widget in seiner Größe eingeschränkt und enthält zwei Nachrichten. Diese zwei Nachrichten entsprechen den zwei neuesten Ereignissen.

Im Widget enthält die Liste der Nachrichten Folgendes:

- Symbol, das dem Thema der Benachrichtigung entspricht: Softwareverteilung ( ), Schutz ( ), Update ( ), Geräteverwaltung ( ), Exploit-Prävention ( ), Administrationsserver ( ).

- Eine Beschreibung der Nachricht mit einem Link zur empfohlenen Maßnahme. Wenn Sie auf den Link klicken und anschließend eine empfohlene Maßnahme durchführen, erhält die Nachricht den Status *Geprüft*.
- Die Anzahl der vergangenen Tage oder Stunden seit die Nachricht auf dem Administrationsserver registriert wurde.
- Ein Link zu weiteren Benachrichtigungen. Durch das Anklicken des Links gelangen Sie in den Unterabschnitt **BENACHRICHTIGUNGEN** des Abschnitts **ÜBERWACHUNG UND BERICHTERSTATTUNG**.

Über die Varianten für den Gerätestatus

Kaspersky Security Center Linux weist jedem verwalteten Gerät einen Status zu. Der jeweilige Status hängt davon ab, ob die vom Benutzer definierten Bedingungen erfüllt sind. Wenn Kaspersky Security Center Linux einem Gerät einen Status zuweist, wird in bestimmten Fällen das Sichtbarkeits-Flag des Gerätes im Netzwerk berücksichtigt (siehe folgende Tabelle). Wenn Kaspersky Security Center Linux ein Gerät innerhalb von zwei Stunden nicht im Netzwerk findet, wird das Sichtbarkeits-Flag des Gerätes auf *Nicht sichtbar* gesetzt.

Es gibt folgende Statusvarianten:

- *Kritisch* oder *Kritisch/Sichtbar*
- *Warnung* oder *Warnung/Sichtbar*
- *OK* oder *OK/Sichtbar*

Die folgende Tabelle enthält die erforderlichen Standardbedingungen, nach denen einem Gerät der Status *Kritisch* oder *Warnung* zugewiesen wird, sowie alle möglichen Werte.

Bedingungen für das Zuweisen der Status an das Gerät

Bedingung	Beschreibung der Bedingung	Mögliche Werte
Es wurde keine Sicherheitsanwendung installiert	Auf dem Gerät ist der Administrationsagent installiert, aber es wurde keine Sicherheitsanwendung installiert.	• Umschalter aktiviert. • Umschalter deaktiviert.
Zu viele Viren gefunden	Auf dem Gerät wurden 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 Untersuchung auf	Das Gerät ist im Netzwerk sichtbar und eine Sicherheits-App wurde auf dem Gerät installiert, aber die Aufgabe "Untersuchung auf Viren" wurde nicht innerhalb des angegebenen Zeitintervalls	Über 1 Tag.

Viren liegt lange zurück	ausgeführt. Die Bedingung gilt nur für Geräte, die vor mehr als sieben Tagen zur Datenbank des Administrationsservers hinzugefügt wurden.	
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 installiert	Das Gerät ist im Netzwerk sichtbar, aber infolge der Inventarisierung der Software durch den Administrationsagenten wurden auf dem Gerät inkompatible Programme gefunden.	• Umschalter deaktiviert. • Umschalter aktiviert.
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.
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 ermöglicht es, den Status eines Gerätes in einer Administrationsgruppe unter bestimmten Bedingungen automatisch zu ändern. Bei Erfüllung der festgelegten Bedingungen wird dem Client-Gerät einer der folgenden Statuswerte verliehen: *Kritisch* oder *Warnung*. Sind die festgelegten Bedingungen nicht erfüllt, so erhält das Client-Gerät den Status *OK*.

Verschiedenen Werten einer einzelnen Bedingung können verschiedene Statusvarianten entsprechen. Beispiele: Wenn die Bedingung **Die Datenbanken sind veraltet** den Wert **Über 3 Tage** besitzt, erhält das Client-Gerät standardmäßig den Status *Warnung*, für den Wert **Über 7 Tage** wird der Status *Kritisch* zugewiesen.

Wenn Sie Kaspersky Security Center Linux von der vorhergehenden Version upgraden, bleiben die Werte für die Zuweisung der Statusvarianten *Kritisch* oder *Warnung* für die Bedingung **Die Datenbanken sind veraltet** unverändert.

Wenn Kaspersky Security Center Linux 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 **Kritisch**.
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 **Uhrzeit der Verschlüsselung**.

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 **Warnung**.
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 **Uhrzeit der Verschlüsselung**.

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Warnung*.

Einstellungen für das Versenden von Benachrichtigungen anpassen

Sie können die Benachrichtigung über Ereignisse, die in Kaspersky Security Center Linux auftreten, konfigurieren. Je nach ausgewählter Benachrichtigungsmethode, stehen die folgenden Benachrichtigungstypen zur Verfügung:

- E-Mail: Wenn Ereignisse auftreten, sendet Kaspersky Security Center Linux Benachrichtigungen an die angegebenen E-Mail-Adressen.

- SMS: Wenn Ereignisse auftreten, sendet Kaspersky Security Center Linux Benachrichtigungen an die angegebenen Telefonnummern.

- Ausführbare Datei: Wählen Sie die ausführbare Datei, die auf dem Administrationsserver gestartet wird, wenn ein Ereignis eintritt.

Um den Versand von Benachrichtigungsereignissen in Kaspersky Security Center Linux zu konfigurieren:

1. Klicken Sie im oberen Bereich des Bildschirms auf das Symbol **Einstellungen** () neben dem Namen des erforderlichen Administrationsservers.

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

2. Klicken Sie auf den Abschnitt **Benachrichtigung**, und wählen Sie im rechten Bereich die Registerkarte für die gewünschte Benachrichtigungsmethode:

   - E-Mail

Auf der Registerkarte **E-Mail** können Sie die Ereignisprotokollierung per E-Mail konfigurieren.

Geben Sie im Feld **SMTP-Server** die Adressen der Mail-Server durch Semikolon getrennt an. Sie können folgende Parameterwerte verwenden:

- IPv4- oder IPv6-Adresse
- DNS-Name des SMTP-Servers

Geben Sie im Feld **Port des SMTP-Servers** die Nummer des Kommunikationsports auf dem SMTP-Server an. Standardmäßig ist Portnummer 25 angegeben.

Wenn Sie die Option **"DNS MX lookup" verwenden** aktivieren, können Sie mehrere MX-Einträge von IP-Adressen für denselben DNS-Namen des SMTP-Servers verwenden. Der gleiche DNS-Name kann mehrere MX-Einträge mit unterschiedlichen Prioritäten für das Empfangen von E-Mail-Nachrichten enthalten. Der Administrationsserver versucht, entsprechend der Priorität der MX-Einträge, die E-Mail-Nachrichten in aufsteigender Reihenfolge an den SMTP-Server zu senden.

Wenn Sie die Option **"DNS MX lookup" verwenden** aktivieren und die Verwendung von TLS-Einstellungen deaktivieren, ist es empfehlenswert, die DNSSEC-Einstellungen auf Ihrem Servergerät als zusätzliche Schutzmaßnahme beim Senden von E-Mail-Nachrichten zu verwenden.

Wenn Sie die Option **ESMTP-Authentifizierung verwenden** aktivieren, können Sie die ESMTP-Authentifizierungseinstellungen in den Feldern **Benutzername** und **Kennwort** angeben. Standardmäßig ist die Option deaktiviert und die ESMTP-Authentifizierungseinstellungen sind nicht verfügbar.

Sie können die TLS-Einstellungen einer Verbindung mit einem SMTP-Server angeben:

- **TLS nicht verwenden**

Sie können diese Option auswählen, wenn Sie die Verschlüsselung von E-Mail-Nachrichten deaktivieren möchten.

- **TLS verwenden, wenn dies vom SMTP-Server unterstützt wird**

Sie können diese Option auswählen, wenn Sie eine TLS-Verbindung zu einem SMTP-Server verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, verbindet der Administrationsserver den SMTP-Server ohne TLS zu verwenden.

- **Immer TLS verwenden, das Serverzertifikat auf Gültigkeit überprüfen**

Sie können diese Option auswählen, wenn Sie Authentifizierungseinstellungen von TLS verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, kann der Administrationsserver keine Verbindung zu dem SMTP-Server herstellen.

Es wird empfohlen, diese Option für einen besseren Schutz der Verbindung mit einem SMTP-Server zu verwenden. Wenn Sie diese Option auswählen, können Sie Authentifizierungseinstellungen für eine TLS-Verbindung festlegen.

Wenn Sie den Wert **Immer TLS verwenden, das Serverzertifikat auf Gültigkeit überprüfen** ausgewählt haben, können Sie ein Zertifikat für die Authentifizierung des SMTP-Servers angeben und auswählen, ob Sie die Kommunikation über eine beliebige Version von TLS oder nur über TLS 1.2 oder höher aktivieren möchten. Außerdem können Sie ein Zertifikat für die Client-Authentifizierung an dem SMTP-Server angeben.

Sie können Zertifikate für eine TLS-Verbindung angeben, indem Sie auf den Link **Zertifikate angeben** klicken:

- Geben Sie eine Datei mit SMTP-Server-Zertifikat an:

Sie können eine Datei bekommen, die eine Liste mit Zertifikaten von eine vertrauenswürdigen Zertifizierungsstelle enthält, und diese Datei auf den Administrationsserver hochladen. Kaspersky Security Center Linux prüft, ob das Zertifikat eines SMTP-Servers auch von einer vertrauenswürdigen Zertifizierungsstelle signiert ist oder nicht. Kaspersky Security Center Linux kann keine Verbindung zu einem SMTP-Server herstellen, wenn das Zertifikat des SMTP-Servers nicht von eine vertrauenswürdigen Zertifizierungsstelle kommt.

- Geben Sie die Datei des Client-Zertifikats an:

Sie können ein Zertifikat verwenden, das Sie von einer beliebigen Quelle erhalten haben, beispielsweise von einer vertrauenswürdigen Zertifizierungsstelle. Sie müssen das Zertifikat und seinen privaten Schlüssel angeben, indem Sie einen der folgenden Zertifikat-Typen verwenden:

- X-509-Zertifikat:

Sie müssen eine Datei mit dem Zertifikat und eine Datei mit dem privaten Schlüssel angeben. Beide Dateien sind unabhängig voneinander und die Reihenfolge für das Laden der Dateien ist spielt keine Rolle. Wenn beide Dateien geladen sind, müssen Sie das Kennwort zum Entschlüsseln des privaten Schlüssels angeben. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

- pkcs12-Container:

Sie müssen eine einzelne Datei hochladen, die das Zertifikat und seinen privaten Schlüssel enthält. Wenn die Datei geladen ist, müssen Sie anschließend das Kennwort zum Entschlüsseln des privaten Schlüssels angeben. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

Wenn Sie auf die Schaltfläche **Testnachricht senden** klicken, können Sie prüfen, ob die Benachrichtigungen korrekt angepasst sind: Das Programm sendet eine Testnachricht an die von Ihnen angegebenen E-Mail-Adressen.

Geben Sie im Feld **Empfänger (E-Mail-Adressen)** die E-Mail-Adressen an, an die das Programm Benachrichtigungen senden soll. Sie können in diesem Feld mehrere Adressen angeben, indem Sie diese durch Semikolons trennen.

Geben Sie im Feld **Betreff** den Betreff der E-Mail an. Sie können dieses Feld leer lassen.

Wählen Sie in der Dropdown-Liste **Betreffsvorlage** die Vorlage für Ihren Betreff aus. Eine durch die ausgewählte Vorlage bestimmte Variable wird automatisch in das Feld **Betreff** eingefügt. Sie können einen E-Mail-Betreff erstellen, indem Sie mehrere Betreffsvorlagen auswählen.

Geben Sie im Feld **E-Mail-Adresse des Absenders: Wenn diese Einstellung nicht angegeben ist, wird stattdessen die Empfängeradresse verwendet. Warnung: Es wird nicht empfohlen, eine fiktive E-Mail-Adresse zu verwenden** die E-Mail-Adresse des Absenders an. Wenn Sie dieses Feld leer lassen, wird standardmäßig die Empfängeradresse verwendet. Wir raten davon ab, fingierte E-Mail-Adressen zu verwenden.

Das Feld **Benachrichtigungstext** enthält Standard-Text mit der Information zum Ereignis, der beim Eintreten des Ereignisses versendet wird. Dieser Text enthält Platzhalter für den Ereignisnamen, den Gerätenamen und den Namen der Domäne. Sie können den Text der Meldung bearbeiten und weitere Platzhalter mit relevanten Informationen zum Ereignis hinzufügen.

Wenn der Benachrichtigungstext ein Prozentzeichen (%) enthält, muss es zweimal hintereinander angegeben werden, damit die Nachricht versendet werden kann. Beispielsweise "Die Prozessor-Auslastung liegt bei 100%%".

Wenn Sie auf den Link **Beschränkung für die Anzahl der Benachrichtigungen konfigurieren** klicken, können Sie die maximale Anzahl an Benachrichtigungen angeben, die das Programm innerhalb des angegebenen Zeitintervalls versenden darf.

- SMS

Auf der Registerkarte **SMS** können Sie den Versand von SMS-Benachrichtigungen zu verschiedenen Ereignissen an ein Mobiltelefon anpassen. SMS-Nachrichten werden über ein Mail-Gateway gesendet.

Geben Sie im Feld **SMTP-Server** die Adressen der Mail-Server durch Semikolon getrennt an. Sie können folgende Parameterwerte verwenden:

- IPv4- oder IPv6-Adresse
- DNS-Name des SMTP-Servers

Geben Sie im Feld **Port des SMTP-Servers** die Nummer des Kommunikationsports auf dem SMTP-Server an. Standardmäßig ist Portnummer 25 angegeben.

Wenn die Option **ESMTP-Authentifizierung verwenden** aktiviert ist, können Sie die ESMTP-Authentifizierungseinstellungen in den Feldern **Benutzername** und **Kennwort** angeben. Standardmäßig ist die Option deaktiviert und die ESMTP-Authentifizierungseinstellungen sind nicht verfügbar.

Sie können die TLS-Einstellungen einer Verbindung mit einem SMTP-Server angeben:

- **TLS nicht verwenden**

Sie können diese Option auswählen, wenn Sie die Verschlüsselung von E-Mail-Nachrichten deaktivieren möchten.

- **TLS verwenden, wenn dies vom SMTP-Server unterstützt wird**

Sie können diese Option auswählen, wenn Sie eine TLS-Verbindung zu einem SMTP-Server verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, verbindet der Administrationsserver den SMTP-Server ohne TLS zu verwenden.

- **Immer TLS verwenden, das Serverzertifikat auf Gültigkeit überprüfen**

Sie können diese Option auswählen, wenn Sie Authentifizierungseinstellungen von TLS verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, kann der Administrationsserver keine Verbindung zu dem SMTP-Server herstellen.

Es wird empfohlen, diese Option für einen besseren Schutz der Verbindung mit einem SMTP-Server zu verwenden. Wenn Sie diese Option auswählen, können Sie Authentifizierungseinstellungen für eine TLS-Verbindung festlegen.

Wenn Sie den Wert **Immer TLS verwenden, das Serverzertifikat auf Gültigkeit überprüfen** ausgewählt haben, können Sie ein Zertifikat für die Authentifizierung des SMTP-Servers angeben und auswählen, ob Sie die Kommunikation über eine beliebige Version von TLS oder nur über TLS 1.2 oder höher aktivieren möchten. Außerdem können Sie ein Zertifikat für die Client-Authentifizierung an dem SMTP-Server angeben.

Sie können die Zertifikatsdatei des SMTP-Servers angeben, indem Sie auf den Link **Zertifikate angeben** klicken. Sie können eine Datei bekommen, die eine Liste mit Zertifikaten von eine vertrauenswürdigen Zertifizierungsstelle enthält, und diese Datei auf den Administrationsserver hochladen. Kaspersky Security Center Linux prüft, ob das Zertifikat eines SMTP-Servers auch von einer vertrauenswürdigen Zertifizierungsstelle signiert ist oder nicht. Kaspersky Security Center Linux kann keine Verbindung zu einem SMTP-Server herstellen, wenn das Zertifikat des SMTP-Servers nicht von eine vertrauenswürdigen Zertifizierungsstelle kommt.

Geben Sie im Feld **Empfänger (E-Mail-Adressen)** die E-Mail-Adressen an, an die das Programm Benachrichtigungen senden soll. Sie können in diesem Feld mehrere Adressen angeben, indem Sie diese durch Semikolons trennen. Die Benachrichtigungen werden an die Telefonnummern gesendet, die den angegebenen E-Mail-Adressen zugewiesen sind.

Geben Sie im Feld **Betreff** den Betreff der E-Mail an.

Wählen Sie in der Dropdown-Liste **Betreffsvorlage** die Vorlage für Ihren Betreff aus. Eine Variable entsprechend der ausgewählten Vorlage wird in das Feld **Betreff** eingefügt. Sie können einen E-Mail-Betreff erstellen, indem Sie mehrere Betreffsvorlagen auswählen.

Geben Sie im Feld **E-Mail-Adresse des Absenders: Wenn diese Einstellung nicht angegeben ist, wird stattdessen die Empfängeradresse verwendet. Warnung: Es wird nicht empfohlen, eine fiktive E-Mail-Adresse zu verwenden** die E-Mail-Adresse des Absenders an. Wenn Sie dieses Feld leer lassen, wird standardmäßig die Empfängeradresse verwendet. Wir raten davon ab, fingierte E-Mail-Adressen zu verwenden.

Geben Sie im Feld **Telefonnummern der SMS-Nachrichtenempfänger** die Mobiltelefonnummern der Empfänger der SMS-Benachrichtigungen ein.

Geben Sie im Feld **Benachrichtigungstext** den Text mit der Information zum Ereignis ein, der beim Eintreten des Ereignisses versendet wird. Dieser Text kann Platzhalter für den Ereignisnamen, den Gerätenamen und den Namen der Domäne enthalten.

Wenn der Benachrichtigungstext ein Prozentzeichen (%) enthält, muss es zweimal hintereinander angegeben werden, damit die Nachricht versendet werden kann. Beispielsweise "Die Prozessor-Auslastung liegt bei 100%%".

Klicken Sie auf **Testnachricht senden**, um zu prüfen, ob Sie die Benachrichtigungen korrekt konfiguriert haben: Das Programm sendet dann eine Testnachricht an die von Ihnen angegebenen Empfänger.

Klicken Sie auf den Link **Beschränkung für die Anzahl der Benachrichtigungen konfigurieren**, um die maximale Anzahl an Benachrichtigungen anzugeben, die das Programm während des angegebenen Zeitintervalls versenden darf.

- **Start einer ausführbaren Datei**

  Wenn diese Methode der Zustellung von Benachrichtigungen ausgewählt ist, können Sie im Eingabefeld das Programm angeben, das gestartet wird, sobald ein Ereignis eintritt.

  Geben Sie im Feld **Ausführbare Datei, die auf dem Administrationsserver gestartet wird, wenn ein Ereignis eintritt** den Ordner und den Namen der auszuführenden Datei an. Bevor Sie die Datei angeben, bereiten Sie die diese vor und geben Sie die Platzhalter an die für die Ereignisdetails stehen, die in der Nachricht gesendet werden sollen. Der von Ihnen angegebene Ordner und die Datei müssen sich auf dem Administrationsserver befinden.

  Wenn Sie auf den Link **Beschränkung für die Anzahl der Benachrichtigungen konfigurieren** klicken, können Sie die maximale Anzahl an Benachrichtigungen angeben, die das Programm innerhalb des angegebenen Zeitintervalls versenden darf.

3. Definieren Sie auf der Registerkarte die Benachrichtigungseinstellungen.
4. Klicken Sie auf die Schaltfläche **Uhrzeit der Verschlüsselung**, 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 Linux auftreten.

Für die Einstellungen des Administrationsservers, einer Richtlinie oder des Programms können Sie im Abschnitt **Konfiguration von Ereignissen** die Benachrichtigungseinstellungen für bestimmte Ereignisse überschreiben.

Verteilung von Benachrichtigungen prüfen

Um zu überprüfen, ob Ereignisbenachrichtigungen versendet werden, verwendet das Programm eine Benachrichtigung über den Fund des Eicar-Testvirus auf den Client-Geräten.

Um die Verteilung von Benachrichtigungen über Ereignisse zu überprüfen, gehen Sie wie folgt vor:

1. Halten Sie auf einem Client-Computer den Echtzeitschutz für das Dateisystem an und kopieren Sie den Eicar-Testvirus auf das Client-Gerät. Aktivieren Sie den Echtzeitschutz für das Dateisystem wieder.

2. Starten Sie eine Untersuchungsaufgabe für die Client-Geräte in einer Administrationsgruppe oder für eine Reihe von Geräten, zu denen das Client-Gerät mit dem Eicar-Testvirus gehört.

   Wenn die Untersuchungsaufgabe richtig konfiguriert ist, wird der Testvirus gefunden. Wurden die Einstellungen für Benachrichtigungen richtig angepasst, empfangen Sie eine Meldung über den gefundenen Virus.

Um einen Eintrag für die Erkennung des Testvirus zu öffnen:

1. Wechseln Sie im Hauptmenü zu **ÜBERWACHUNG UND BERICHTERSTATTUNG → EREIGNISAUSWAHLEN**.

2. Klicken Sie auf den Namen der Auswahl **Letzte Ereignisse**.

   Im angezeigten Fenster wird die Benachrichtigung über den Testvirus angezeigt.

Der Eicar-Testvirus enthält keinen Programmcode, der Ihrem Gerät Schaden zufügen könnte. Die Sicherheits-Apps der meisten Hersteller identifizieren ihn aber als Virus. Der Testvirus steht auf der offiziellen EICAR-Website zum Download bereit.

Benachrichtigung über Ereignisse mithilfe einer ausführbaren Datei

Kaspersky Security Center Linux bietet die Möglichkeit, den Administrator durch den Start einer ausführbaren Datei über Ereignisse auf den Client-Geräten zu benachrichtigen. Diese ausführbare Datei muss eine weitere ausführbare Datei mit Parameterplatzhaltern für das Ereignis enthalten, die dem Administrator übermittelt werden müssen.

Parameterplatzhalter zur Beschreibung des Ereignisses

Parameterplatzhalter	Beschreibung des Parameterplatzhalters
%SEVERITY%	Ereigniskategorie
%COMPUTER%	Name des Geräts, auf dem das Ereignis eingetreten ist
%DOMAIN%	Domäne
%EVENT%	Ereignis
%DESCR%	Ereignisbeschreibung
%RISE_TIME%	Zeitpunkt des Auftretens
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Aufgabenname
%KL_PRODUCT%	Administrationsagent für Kaspersky Security Center Linux
%KL_VERSION%	Versionsnummer des Administrationsagenten
%HOST_IP%	IP-Adresse
%HOST_CONN_IP%	IP-Adresse der Verbindung

Beispiel:

Ausführbare Datei zur Benachrichtigung über Ereignisse (z. B. script1.bat), innerhalb der eine weitere ausführbare Datei (z. B. script2.bat) mit dem Parameterplatzhalter %COMPUTER% gestartet wird. Beim Auftreten eines Ereignisses auf dem Gerät des Administrators wird die Datei script1.bat gestartet, die wiederum die Datei script2.bat mit dem Parameter %COMPUTER% startet. Dadurch erhält der Administrator den Namen des Geräts, auf dem das Ereignis aufgetreten ist.

Kaspersky-Mitteilungen

In diesem Abschnitt wird beschrieben, wie Sie Kaspersky-Mitteilungen verwenden, konfigurieren und deaktivieren.

Über Kaspersky-Mitteilungen

Im Abschnitt mit den Kaspersky-Mitteilungen (**ÜBERWACHUNG UND BERICHTERSTATTUNG → Mitteilungen von Kaspersky**) finden Sie Wissenswertes zu Ihrer Version von Kaspersky Security Center und den verwalteten Programmen, die auf den verwalteten Geräten installiert sind. Kaspersky Security Center aktualisiert die Informationen in diesem Abschnitt regelmäßig: Veraltete Mitteilungen werden entfernt und neue Informationen hinzugefügt.

Kaspersky Security Center zeigt nur die Kaspersky-Mitteilungen an, die sich auf den derzeit verbundenen Administrationsserver und die auf dessen verwalteten Geräten installierten Kaspersky-Programme beziehen. Die Mitteilungen werden für jeden Typ von Administrationsserver individuell angezeigt – primär, sekundär oder virtuell.

Der Administrationsserver benötigt eine Internetverbindung, um Kaspersky-Mitteilungen zu empfangen.

Durch 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. Die Kaspersky-Mitteilungen sind standardmäßig aktiviert. Wenn Sie keine Mitteilungen erhalten möchten, können Sie diese Funktion deaktivieren.

Um Ihnen die Informationen anzuzeigen, die Ihrer Netzwerkschutzkonfiguration entsprechen, sendet Kaspersky Security Center Daten an die Kaspersky-Cloud-Server und empfängt nur die Mitteilungen, welche die in Ihrem Netzwerk installierten Kaspersky-Programme betreffen. Der Datensatz, der an die Server gesendet werden kann, ist im Endbenutzer-Lizenzvertrag beschrieben, den Sie bei der Installation des Kaspersky Security Center Administrationsservers akzeptieren.

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 14 Web Console ein Benachrichtigungssymbol, welches der Ereigniskategorie der Mitteilungen entspricht. Sie können auf das Symbol klicken, um sich die Mitteilung im Abschnitt "Mitteilungen von Kaspersky" anzusehen.

Sie können die Einstellungen für Kaspersky-Mitteilungen konfigurieren, die Mitteilungskategorien wählen, die Sie ansehen möchten, und festlegen, wo das Benachrichtigungssymbol angezeigt werden soll. Wenn Sie keine Mitteilungen erhalten möchten, können Sie diese Funktion deaktivieren.

Einstellungen für die Kaspersky-Mitteilungen angeben

Im Abschnitt Mitteilungen von Kaspersky können Sie die Einstellungen für Kaspersky-Mitteilungen konfigurieren, die Mitteilungskategorien wählen, die Sie ansehen möchten, und festlegen, wo das Benachrichtigungssymbol angezeigt werden soll.

So konfigurieren Sie die Mitteilungen von Kaspersky:

1. Wechseln Sie im Hauptmenü zu **ÜBERWACHUNG UND BERICHTERSTATTUNG → MITTEILUNGEN VON KASPERSKY**.
2. Klicken Sie auf den Link **Einstellungen**.

   Das Fenster mit den Einstellungen für die Kaspersky-Mitteilungen wird geöffnet.
3. Legen Sie die folgenden Einstellungen fest:

   - Wählen Sie die Ereigniskategorie der Mitteilungen, die Sie ansehen möchten. Die Mitteilungen anderer Kategorien werden nicht angezeigt.
   - Geben Sie an, wo das Benachrichtigungssymbol angezeigt werden soll. Das Symbol kann in allen Abschnitt der Konsole, sowie im Abschnitt **ÜBERWACHUNG UND BERICHTERSTATTUNG** und in dessen Unterabschnitten angezeigt werden.
4. Klicken Sie auf die Schaltfläche **OK**.

   Die Einstellungen der Kaspersky-Mitteilungen sind angegeben.

Kaspersky-Mitteilungen deaktivieren

Im Abschnitt Mitteilungen von Kaspersky (**ÜBERWACHUNG UND BERICHTERSTATTUNG → Mitteilungen von Kaspersky**) finden Sie Wissenswertes zu Ihrer Version von Kaspersky Security Center und den verwalteten Programmen, die auf den verwalteten Geräten installiert sind. Wenn Sie keine Mitteilungen von Kaspersky erhalten möchten, können Sie diese Funktion deaktivieren.

Um Kaspersky-Mitteilungen zu deaktivieren:

1. Klicken Sie im Hauptfenster der Anwendung neben dem Namen des benötigten Administrationsservers auf das Symbol **Einstellungen** ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Mitteilungen von Kaspersky** aus.
3. Stellen Sie die Umschaltfläche auf die Position **Sicherheitsrelevante Mitteilungen sind deaktiviert**.
4. Klicken Sie auf die Schaltfläche **Speichern**.

   Jetzt sind die Kaspersky-Mitteilungen deaktiviert.

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

Kaspersky Security Center Linux ermöglicht die Konfiguration des Ereignisexports in SIEM-Systeme. Dafür gibt es folgende Methoden: Export in ein beliebiges SIEM-System, das das Syslog-Format verwendet, oder Export von Ereignissen in SIEM-Systeme direkt aus der Kaspersky Security Center-Datenbank. Nach Abschluss dieses Szenarios sendet der Administrationsserver automatisch Ereignisse an ein SIEM-System.

Erforderliche Komponenten

Bevor Sie mit der Konfiguration des Ereignisexports in Kaspersky Security Center Linux beginnen:

- Erfahren Sie mehr über die Exportmethoden.
- Stellen Sie sicher, dass Sie die Werte der Systemeinstellungen kennen.

> Sie können die Schritte in diesem Szenario in beliebiger Reihenfolge ausführen.

Der Vorgang des Ereignisexports in ein SIEM-System umfasst die folgenden Schritte:

- **Konfigurieren des SIEM-Systems, sodass es Ereignisse aus Kaspersky Security Center empfängt**

  Anleitung: Einstellungen für den Ereignisexport in das SIEM-System

- **Auswählen der Ereignisse, die Sie in das SIEM-System exportieren möchten**

  Markieren der Ereignisse, die Sie in das SIEM-System exportieren möchten. Markieren Sie zuerst die allgemeinen Ereignisse, die in allen verwalteten Kaspersky-Apps auftreten. Dann können Sie die Ereignisse für bestimmte verwaltete Kaspersky-Apps markieren.

- **Konfigurieren des Exports von Ereignissen in das SIEM-System**

  Der Export von Ereignissen kann auf folgende Weisen erfolgen:

  - Über die Protokolle TCP/IP, UDP oder TLS over TCP
  - Mittels direktem Export von Ereignissen aus der Datenbank von Kaspersky Security Center (In der Datenbank von Kaspersky Security Center ist eine Auswahl an öffentlichen Ansichten verfügbar. Die Beschreibung dieser Ansichten finden Sie im Dokument klakdb.chm.)

Ergebnisse

Nach der Konfiguration des Ereignisexports in ein SIEM-System, können Sie sich die Exportergebnisse ansehen, wenn Sie zu exportierende Ereignisse ausgewählt haben.

Vorläufige Bedingungen

Wenn Sie den automatischen Ereignisexport in Kaspersky Security Center Linux einrichten, müssen Sie einige Einstellungen des SIEM-Systems angeben. Es ist empfehlenswert, diese Einstellungen im Voraus zu bestimmen, damit die Einstellungen für Kaspersky Security Center Linux 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 Linux und dem Server des SIEM-Systems hergestellt wird. Dieser Wert muss in den Einstellungen von Kaspersky Security Center Linux und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

- **Protokoll**

  Das Protokoll, das für die Übertragung von Daten aus Kaspersky Security Center Linux ins SIEM-System verwendet wird. Dieser Wert muss in den Einstellungen von Kaspersky Security Center Linux und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

Über Ereignisse in Kaspersky Security Center Linux

Kaspersky Security Center Linux 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 Linux 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 von Kaspersky Security Center Linux:
  - 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 eine Speicherdauer festgelegt, die in Kaspersky Security Center Linux 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.

Über den Ereignisexport

Sie können den Ereignisexport innerhalb zentralisierten Systemen verwenden, die sich mit Fragen der Sicherheit auf organisatorischer und technischer Ebene und der Überwachung des Sicherheitssystems beschäftigen sowie Daten aus verschiedenen Lösungen konsolidieren. Dazu gehören SIEM-Systeme, die eine Analyse der Warnungen der Sicherheitssysteme und Ereignisse der Netzwerkhardware und 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 Linux in externe SIEM-Systeme sind zwei Seiten beteiligt: der Absender der Ereignisse (Kaspersky Security Center Linux) und der Empfänger der Ereignisse (ein SIEM-System). Für einen erfolgreichen Ereignisexport müssen die Einstellungen sowohl im verwendeten SIEM-System als auch in Kaspersky Security Center Linux angepasst werden. Die Reihenfolge der Einstellungen hat keine Bedeutung: Sie können entweder zuerst den Versand der Ereignisse in Kaspersky Security Center Linux 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 Linux übertragenen Ereignisse übernehmen und korrekt analysieren. Dazu müssen die Einstellungen des SIEM-Systems angepasst werden. Die Konfiguration hängt vom verwendeten speziellen SIEM-System ab. Es gibt jedoch eine Anzahl von allgemeinen Schritten in der Konfiguration aller SIEM-Systeme, etwa die Konfiguration des Empfängers und des Parsers.

Über das Konfigurieren des Ereignisexports in ein SIEM-System

Am Ablauf des Ereignisexports aus Kaspersky Security Center Linux in externe SIEM-Systeme sind zwei Seiten beteiligt: der Absender der Ereignisse (Kaspersky Security Center Linux) und der Empfänger der Ereignisse (ein SIEM-System). Sie müssen den Ereignisexport im verwendeten SIEM-System und in Kaspersky Security Center Linux anpassen.

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 Linux gesendet werden, angepasst werden. Im Allgemeinen müssen im SIEM-System die folgenden Einstellungen angegeben werden:

- **Exportprotokoll**

  Ein Protokoll zum Übertragen von Nachrichten, entweder UDP, TCP oder TLS over TCP. Es muss dasselbe Protokoll angegeben werden wie in Kaspersky Security Center Linux.

- **Port**

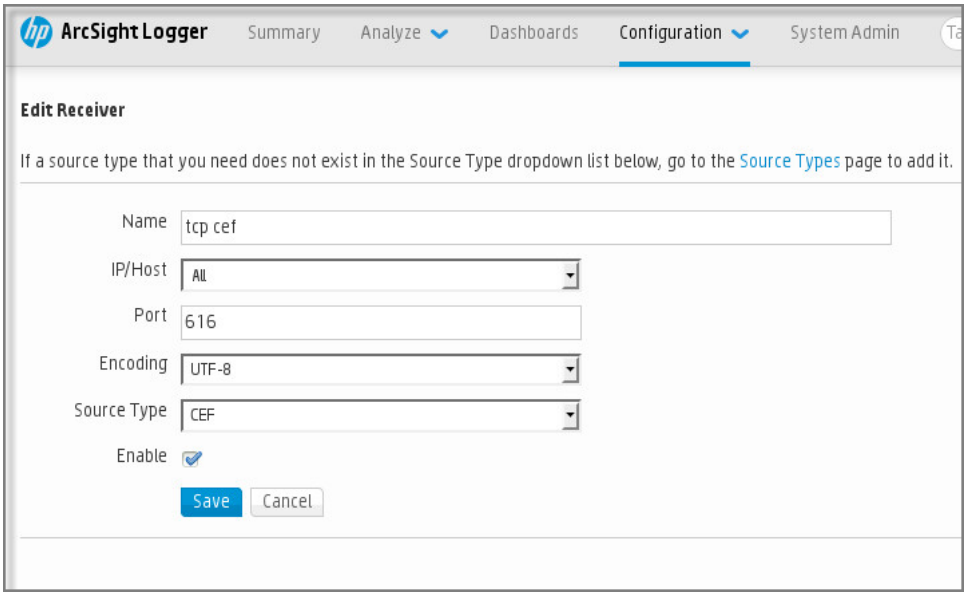
Geben Sie die Portnummer für die Verbindung mit Kaspersky Security Center Linux an. Dieser Port muss derselbe sein wie der Port, den Sie in Kaspersky Security Center Linux bei der Konfiguration für das SIEM-System angeben.

- **Datenformat**

  Geben Sie das Syslog-Format an.

Je nachdem, welches SIEM-System Sie verwendetem, kann es erforderlich sein, erweiterte Einstellungen für den Empfänger der Nachrichten anzugeben.

Auf der unteren Abbildung dienen die Einstellungen des Empfängers in ArcSight als Beispiel.



Einstellungen des Empfängers in ArcSight

Nachrichtenparser

Die exportierten Ereignisse werden in Form von Nachrichten an das SIEM-System übergeben. Dann wird für diese Nachrichten der Parser verwendet, damit die Informationen über die Ereignisse entsprechend ins SIEM-System übergeben werden. Die Nachrichtenparser sind im SIEM-System integriert; sie werden für die Aufteilung der Nachrichten in Felder, etwa ID der Nachricht, Ereigniskategorie, Beschreibung und die übrigen Einstellungen verwendet. Dadurch hat das SIEM-System die Möglichkeit, die Ereignisse, die aus Kaspersky Security Center Linux 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 von Kaspersky bereitgestellten Parser.

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 auswählen, welche Ereignisse ins externe SIEM-System exportiert werden sollen.

Sie können den Ereignisexport in das Syslog-Format in ein externes System gemäß einer der folgenden Bedingungen anpassen:

- Allgemeine Ereignisse markieren. Wenn Sie die zu exportierenden Ereignisse in der Richtlinie, in den Einstellungen eines Ereignisses oder in den Einstellungen des Administrationsservers markieren, erhält das SIEM-System die ausgewählten Ereignisse, die in allen 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 auf das Symbol **Einstellungen** (🔧) neben dem Namen des benötigten Administrationsservers.
   - 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 Linux in externe Systeme verwendet.

In Kaspersky Security Center Linux können Sie den Ereignisexport in externe Systeme unter Verwendung des Syslog-Formats anpassen.

Der Ablauf des Exports besteht aus zwei Schritten:

1. Aktivierung des automatischen Ereignisexports. In diesem Schritt werden die Einstellungen von Kaspersky Security Center Linux so angepasst, dass der Versand von Ereignissen ins SIEM-System ausgeführt werden kann. Der Versand von Ereignissen aus Kaspersky Security Center Linux 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 Linux für den Export von Ereignissen in ein SIEM-System

Um Ereignisse an ein SIEM-System zu exportieren müssen Sie den Exportprozess in Kaspersky Security Center Linux konfigurieren.

So konfigurieren Sie den Export in SIEM-Systeme in Kaspersky Security Center 14 Web Console:

1. Wählen Sie in der Dropdown-Liste **Konsolen-Einstellungen** die Option **Integration**.

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

2. Wählen Sie die Registerkarte **Integration** aus.

3. Wählen Sie auf der Registerkarte **Integration** den Abschnitt **SIEM** aus.

4. Klicken Sie auf den Link **Einstellungen**.

   Der Abschnitt **Einstellungen exportieren** wird geöffnet.

5. 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 Linux und dem Server des SIEM-Systems hergestellt wird. Dieser Wert muss in den Einstellungen von Kaspersky Security Center Linux und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

   - **Protokoll**

Wählen Sie das Übertragungsprotokoll für Nachrichten ins SIEM-System aus. Sie können entweder die Protokolle TCP/IP, UDP oder TLS over TCP auswählen.

Wenn Sie das Protokoll TLS over TCP auswählen, geben Sie die folgenden TLS-Einstellungen an:

- **Authentifizierung des Servers**

  In dem Feld **Authentifizierung des Servers** können Sie die **Vertrauenswürdige Zertifikate** oder Werte der **SHA-Fingerabdrücke** auswählen:

  - **Vertrauenswürdige Zertifikate**. Sie können eine Datei bekommen, die eine Liste mit Zertifikaten von einer vertrauenswürdigen Zertifizierungsstelle (Certification Authority – CA) enthält, und diese Datei in Kaspersky Security Center Liste hochladen. Kaspersky Security Center Linux 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**. In Kaspersky Security Center können Sie die SHA-1-Fingerabdrücke der Zertifikate von SIEM-Systemen angeben. Um einen SHA-1-Fingerabdruck hinzuzufügen, geben Sie ihn in das Feld **Fingerabdrücke** ein und klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

  Durch Verwendung der Einstellung **Client-Authentifizierung hinzufügen** können Sie ein Zertifikat generieren, um Kaspersky Security Center zu authentifizieren. Infolge dessen verwenden Sie ein selbstsigniertes Zertifikat, das von Kaspersky Security Center ausgestellt wurde. In diesem Fall können Sie sowohl ein vertrauenswürdiges Zertifikat als auch einen SHA-Fingerabdruck verwenden, um den SIEM-Systemserver zu authentifizieren.

- **Namen des Antragstellers/des alternativen Antragstellers hinzufügen**

  Der Antragstellername ist ein Domänenname, für den das Zertifikat empfangen wird. Kaspersky Security Center Linux 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 **Namen des Antragstellers/des alternativen Antragstellers hinzufügen** angeben. Wenn einer der angegebenen Antragstellernamen mit dem Antragsteller des Zertifikats für das SIEM-Systems übereinstimmt, validiert Kaspersky Security Center Linux das Zertifikat dieses SIEM-Systems.

- **Client-Authentifizierung hinzufügen**

  Um die Client-Authentifizierung durchzuführen, können Sie entweder Ihr Zertifikat einfügen oder es im Kaspersky Security Center generieren.

  - **Zertifikat einfügen**. Sie können ein Zertifikat verwenden, das Sie von einer beliebigen Quelle erhalten haben, beispielsweise von einer vertrauenswürdigen CA. Sie müssen das Zertifikat und seinen privaten Schlüssel angeben, indem Sie einen der folgenden Zertifikat-Typen verwenden:

    - **X.509-Zertifikat PEM**. Laden Sie jeweils eine Datei mit Zertifikat über das Feld **Datei mit Zertifikat** und eine Datei mit privatem Schlüssel über das Feld **Datei mit Schlüssel** hoch. Beide Dateien sind unabhängig voneinander und die Reihenfolge für das Hochladen der Dateien ist spielt keine Rolle. Wenn beide Dateien hochgeladen sind, geben Sie das Kennwort zum Entschlüsseln des privaten Schlüssels in dem Feld **Überprüfung von Kennwort oder Zertifikat** an. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

- **X.509-Zertifikat PKCS12**. Laden Sie in dem Feld **Datei mit Zertifikat** eine Datei hoch, die ein Zertifikat und dessen privaten Schlüssel enthält. Geben Sie nach dem Hochladen der Datei das Kennwort zum Entschlüsseln des privaten Schlüssels in dem Feld **Überprüfung von Kennwort oder Zertifikat** an. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

- **Schlüssel generieren**. Sie können in Kaspersky Security Center ein selbstsigniertes Zertifikat generieren. Infolge dessen speichert Kaspersky Security Center Linux das generierte selbstsignierte Zertifikat und Sie können den öffentlichen Teil des Zertifikats oder den SHA1-Fingerabdruck an das SIEM-System übergeben.

6. 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 **Uhrzeit der Verschlüsselung**.

7. Setzen Sie die Option auf die Position **Auto-Exportieren von Ereignissen in die Datenbank des SIEM-Systems Aktiviert**.

8. 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.

Ereignisexport direkt aus der Datenbank

Sie können die Ereignisse direkt aus der Datenbank von Kaspersky Security Center Linux extrahieren, ohne die Benutzeroberfläche von Kaspersky Security Center Linux zu verwenden. Die Abfragen können unmittelbar in Bezug auf die öffentlichen Ansichten erstellt und von daraus Daten über die Ereignisse extrahiert werden, oder Sie können eigene Ansichten auf der Grundlage der vorhandenen öffentlichen Ansichten erstellen und die gewünschten Daten von dort beziehen.

Öffentlichen Ansichten

Zur Erhöhung der Benutzerfreundlichkeit enthält die Datenbank von Kaspersky Security Center Linux einen Satz mit öffentlichen Ansichten. Eine Beschreibung der öffentlichen Ansichten finden Sie im Dokument klakdb.chm.

Die öffentliche Ansicht v_akpub_ev_event enthält einen Satz Felder, die den Einstellungen der Ereignisse in der Datenbank entsprechen. Im Dokument klakdb.chm finden Sie Informationen über die öffentlichen Ansichten, die sich auf andere Objekte von Kaspersky Security Center Linux beziehen, beispielsweise Geräte, Programme oder Benutzer. Sie können diese Informationen beim Erstellen von Abfragen verwenden.

In diesem Abschnitt finden Sie Anweisungen zum Erstellen einer SQL-Abfrage mithilfe des Tools klsql2 sowie ein Beispiel einer solchen Anfrage.

Sie können auch beliebige andere Datenbankenanwendungen für das Erstellen der SQL-Abfragen und die Datenbankenansichten verwenden. Informationen zum Anzeigen der Einstellungen für die Verbindung mit der Datenbank von Kaspersky Security Center Linux (z. B. Instanz-Name und Name der Datenbank) finden Sie im entsprechenden Abschnitt.

Erstellen einer SQL-Abfrage mithilfe des Tools klsql2

In diesem Abschnitt erhalten Sie Anweisungen zum Herunterladen und für die Nutzung des Tools klsql2 sowie zum Erstellen einer SQL-Abfrage mithilfe dieses Tools. Beim Erstellen einer SQL-Abfrage mithilfe des Tools klsql2 müssen Sie den Namen und die Zugriffseinstellungen für die Datenbank nicht angeben, da sich die Abfrage direkt an die öffentlichen Ansichten von Kaspersky Security Center Linux wendet.

Um das Tool klsql2 herunterzuladen und zu verwenden, gehen Sie wie folgt vor:

1. Laden Sie das Tool klsql2 von der Website von Kaspersky herunter.
2. Kopieren Sie den Inhalt des Archives klsql2.zip in einen beliebigen Ordner auf dem Computer, auf dem der Kaspersky Security Center Linux Administrationsserver installiert ist.

   Das Paket klsql2.zip enthält folgende Dateien:

   - klsql2.exe
   - src.sql
   - start.cmd
3. Öffnen Sie die Datei src.sql in einem beliebigen Texteditor.
4. Geben Sie in die src.sql-Datei den von Ihnen gewünschten SQL-Query ein und speichern Sie die Datei.
5. Geben Sie auf dem Computer, auf dem der Kaspersky Security Center Linux Administrationsserver installiert ist, in der Befehlszeile den folgenden Befehl für den Start der SQL-Abfrage aus der Datei src.sql und die Speicherung der Ergebnisse in der Datei result.xml ein:
   ```
   klsql2 -i src.sql -o result.xml
   ```
6. Öffnen Sie die erstellte Datei result.xml und sehen Sie sich die Ergebnisse der Abfragenausführung an.

Sie können die Datei src.sql editieren und darin beliebige Anfragen der öffentlichen Ansichten erstellen. Die Abfragen können dann mithilfe eines Befehls in der Befehlszeile ausgeführt und die Ergebnisse in einer Datei gespeichert werden.

Beispiel einer SQL-Abfrage, die mithilfe des Tools klsql2 erstellt wurde

In diesem Abschnitt ist als Beispiel eine SQL-Anfrage angeführt, die mithilfe des Tools klsql2 erstellt wurde.

Das folgende Beispiel zeigt, wie Sie eine Ereignisliste für die Ereignisse der letzten sieben Tage auf den Geräten der Benutzer erhalten und diese nach der Uhrzeit sortieren, zu der das Ereignis aufgetreten ist, wobei die aktuellsten Ereignisse zuerst angezeigt werden.

Beispiel:
```
SELECT
```

```
e. nId, /* ID des Ereignisses */
e. tmRiseTime, /* Uhrzeit, zu der das Ereignis aufgetreten ist */
e. strEventType, /* interner Name des Ereignistyps */
e. wstrEventTypeDisplayName, /* angezeigter Name des Ereignisses */
e. wstrDescription, /* angezeigte Beschreibung des Ereignisses */
e. wstrGroupName, /* Name der Gerätegruppe */
h.wstrDisplayName, /* angezeigter Gerätename des Geräts, auf dem das Ereignis
aufgetreten ist */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp /* IP-Adresse des Geräts, auf dem das
Ereignis aufgetreten ist */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Anzeige des Namens der Datenbank von Kaspersky Security Center Linux

Falls Sie mithilfe von Datenbankverwaltungssystemen für SQL Server, MySQL oder MariaDB auf die Datenbank von Kaspersky Security Center Linux zugreifen möchten, muss der Name der Datenbank bekannt sein, um sie aus dem SQL-Skript-Editor zu verbinden.

Um den Namen der Datenbank von Kaspersky Security Center Linux anzuzeigen:

1. Klicken Sie auf das Symbol **Einstellungen** () neben dem Namen des benötigten Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Gehen Sie zur Registerkarte **Allgemein** und wählen Sie den Abschnitt **Details der aktuellen Datenbank** aus.

Der Datenbankname wird im Feld **Name der Datenbank** angegeben. Verwenden Sie diesen Namen der Datenbank für die Verbindung und den Zugriff auf die Datenbank in Ihren SQL-Abfragen.

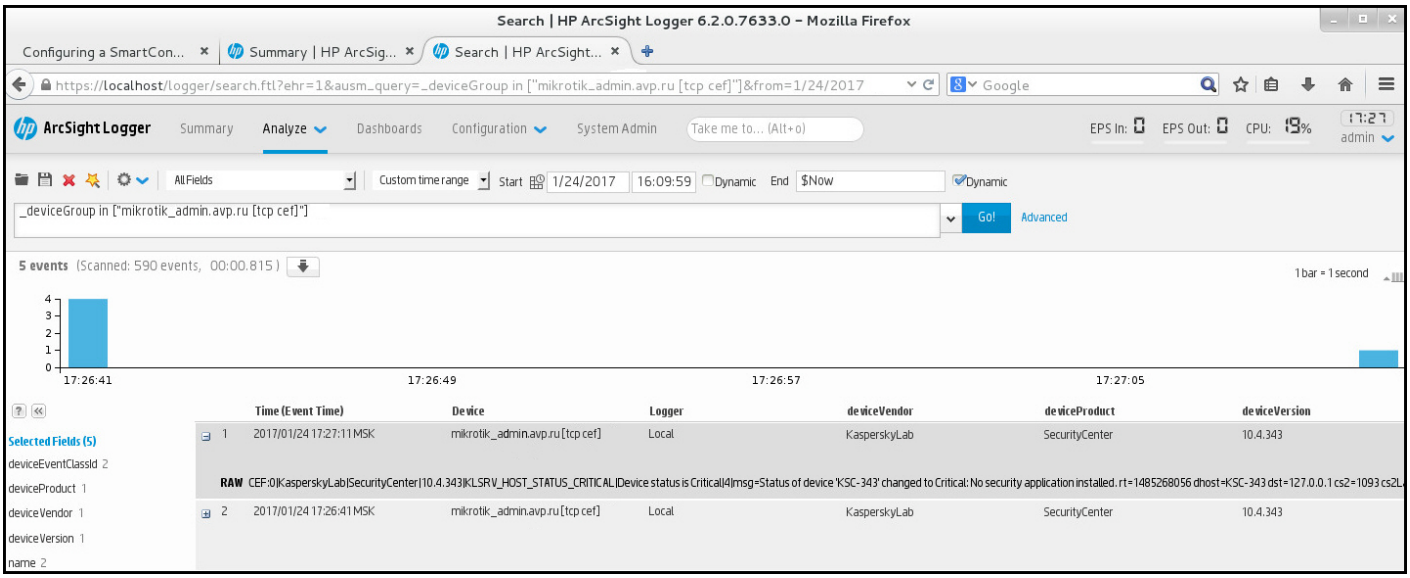
Exportergebnisse anzeigen

Sie können erfahren, ob die Exportprozedur erfolgreich fertig gestellt wurde. Überprüfen Sie dazu, ob das SIEM-System die Nachrichten, in denen die exportierten Ereignisse enthalten sind, erhalten hat.

Wenn die aus Kaspersky Security Center Linux versendeten Ereignisse erhalten und vom SIEM-System richtig interpretiert wurden, bedeutet das, dass die Konfiguration auf beiden Seiten korrekt ausgeführt wurde. Andernfalls prüfen Sie und korrigieren Sie erforderlichenfalls die Einstellungen in Kaspersky Security Center Linux und im SIEM-System.

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

Geräteauswahlen

Geräteauswahlen sind ein Instrument zum Filtern von Geräten nach festgelegten Bedingungen. Sie können Geräteauswahlen verwenden, um mehrere Geräte zu verwalten: beispielsweise, um einen Bericht über nur diese Geräte anzuzeigen, oder um alle diese Geräte in eine andere Gruppe zu verschieben.

Kaspersky Security Center bietet eine große Zahl an *vordefinierten Auswahlen* an (z. B. **Geräte mit dem Status "Kritisch"**, **Der Schutz ist deaktiviert**, **Aktive Bedrohungen werden erkannt**). Vordefinierte Auswahlen können nicht gelöscht werden. Sie können auch zusätzliche *benutzerdefinierte Auswahlen* 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.

Um die Geräteauswahl anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zum Abschnitt **GERÄTE → GERÄTEAUSWAHLEN** or **GERÄTESUCHE UND SOFTWAREVERTEILUNG → GERÄTEAUSWAHLEN**.

2. Klicken Sie in der Auswahlliste auf den Namen der entsprechenden Auswahl.

Das Ergebnis der Geräteauswahl wird angezeigt.

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 den Typ der Geräte an, die Sie in die Geräteauswahl aufnehmen wollen.

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 **Uhrzeit der Verschlüsselung**.

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. Gehen Sie zu **GERÄTE → GERÄTEAUSWAHLEN**.

   Eine Seite mit einer Liste von Geräteauswahlen wird angezeigt.

2. Klicken Sie auf die relevante benutzerdefinierte Geräteauswahl.

   Das Fenster **Einstellungen der Geräteauswahl** wird geöffnet.

3. Geben Sie auf der Registerkarte **Allgemein** Bedingungen an, die erfüllt sein müssen, damit Geräte in die Auswahl aufgenommen werden.

4. 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.

Netzwerk

Im Abschnitt **Netzwerk** können Sie die Bedingungen für die Aufnahme von Geräten anhand ihrer Netzwerkdaten konfigurieren:

- **Gerätename oder IP-Adresse**
- Windows-Domäne

  Es werden alle Geräte angezeigt, die zur angegebenen Arbeitsgruppe gehören.

- Administrationsgruppe

  Es werden Geräte angezeigt, die zur angegebenen Administrationsgruppe gehören.

- Beschreibung

Text im Eigenschaftenfenster des Gerätes: im Feld **Beschreibung** von Abschnitt **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:

    Um Phrasen wie **SUSE Linux Enterprise-Server 12** oder **SUSE Linux Enterprise-Server 15** zu beschreiben, können Sie **SUSE Linux Enterprise-Server 1?** eingeben.

    Das Zeichen ***** oder **?** kann nicht als das erste Zeichen in einer Textbeschreibung verwendet werden.

- Zur Verknüpfung mehrerer Wörter:
  - Leerzeichen: Es werden alle Geräte angezeigt, deren Beschreibung ein beliebiges der angegebenen Wörter enthält.

    Beispiel:

    Zur Beschreibung einer Phrase, die entweder das Wort **Sekundär** oder **Virtuell** enthält, können Sie die Zeichenfolge **Sekundär Virtuell** verwenden.

  - **+**: Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort unbedingt im Text vorhanden sein muss.

    Beispiel:

    Zur Beschreibung einer Phrase, welche die beiden Wörter **Sekundär** und **Virtuell** enthält, können Sie den Ausdruck **+Sekundär+Virtuell** verwenden.

  - **-**: Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort im Suchtext nicht vorkommen darf.

    Beispiel:

    Zur Beschreibung einer Phrase, die das Wort **Sekundär** enthält, jedoch das Wort **Virtuell** nicht enthalten darf, können Sie den Ausdruck **+Sekundär-Virtuell** verwenden.

  - **"<Textabschnitt>"**: Ein in Anführungszeichen eingeschlossener Textabschnitt muss vollständig im Text vorhanden sein.

    Beispiel:

    Zur Beschreibung einer Phrase, welche die Wortverbindung **Sekundärer Server** enthält, können Sie den Ausdruck **"Sekundärer Server"** verwenden.

- IP-Bereich

Wenn diese Option aktiviert ist, können Sie in den Eingabefeldern die erste und die letzte IP-Adresse des Bereichs eingeben, zu dem die betreffenden Geräte gehören sollen.

Diese Option ist standardmäßig deaktiviert.

Tags

Im Abschnitt **Tags** können Sie Bedingungen für die Aufnahme von Geräten in die Auswahl nach Schlüsselworten (Tags) anpassen, die zuvor zu den Beschreibungen der verwalteten Geräte hinzugefügt wurden:

- Anwenden, wenn mindestens eins der ausgewählten Tags zutrifft

  Ist die Option aktiviert, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibungen zumindest einer der gewählten Tags vorhanden ist.

  Ist die Option deaktiviert, werden in den Suchergebnissen nur Geräte angezeigt, in deren Beschreibungen alle gewählten Tags vorhanden sind.

  Diese Option ist standardmäßig deaktiviert.

- Der Tag muss vorhanden sein

  Wenn diese Variante ausgewählt ist, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibung der ausgewählte Tag vorhanden ist. Bei der Gerätesuche können Sie das Zeichen * verwenden, um eine beliebige Zeile mit einer beliebigen Anzahl von Zeichen zu ersetzen.

  Diese Variante ist standardmäßig ausgewählt.

- Der Tag darf nicht vorhanden sein

  Wenn diese Variante ausgewählt ist, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibung der ausgewählte Tag nicht vorhanden ist. Bei der Gerätesuche können Sie das Zeichen * verwenden, um eine beliebige Zeile mit einer beliebigen Anzahl von Zeichen zu ersetzen.

Netzwerkaktivität

Im Abschnitt **Netzwerkaktivität** können Sie die Bedingungen für die Aufnahme von Geräten anhand ihrer Netzwerkaktivitäten konfigurieren:

- Dieses Gerät ist ein Verteilungspunkt

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Ja**. Bei Auswahl dieser Option werden Geräte, die als Verteilungspunkte fungieren, in die Auswahl aufgenommen.
  - **Nein**. Geräte, die als Verteilungspunkte fungieren, werden nicht in die Auswahl aufgenommen.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- Verbindung mit Administrationsserver nicht trennen

In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

- **Aktiviert**. Zur Auswahl gehören die Geräte, auf denen das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen** aktiviert ist.
- **Deaktiviert**. Zur Auswahl gehören die Geräte, auf denen das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen** deaktiviert ist.
- **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- 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.

Programm

Im Abschnitt **Programm** können Sie die Kriterien für die Aufnahme von Geräten anhand des ausgewählten verwalteten Programms konfigurieren:

- Programmname

  In der Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl wählen, wenn die Suche anhand des Namens 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

  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.

- Letztes Update der Module

  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 verwaltet

Mithilfe dieser Dropdown-Liste können Geräte in die Auswahl aufgenommen werden, die über Kaspersky Security Center Linux verwaltet werden:

- **Ja**. Geräte werden in die Auswahl aufgenommen, wenn sie über Kaspersky Security Center Linux verwaltet werden.
- **Nein**. Das Programm nimmt Geräte in die Auswahl auf, wenn sie nicht über Kaspersky Security Center Linux verwaltet werden.
- **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- Es wurde eine Sicherheitsanwendung 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.

Betriebssystem

Im Abschnitt **Betriebssystem** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl auf der Grundlage des darauf installierten Betriebssystems anpassen.

- Version des Betriebssystems

  Ist das Kontrollkästchen aktiviert, können Sie Betriebssysteme in der Liste auswählen. Geräte, auf denen die angegebenen Betriebssysteme installiert sind, werden in die Suchergebnisse aufgenommen.

- Bitzahl des Betriebssystems

  In dieser Dropdown-Liste können Sie die Architektur des Betriebssystems auswählen, die vorhanden sein muss, damit auf dem Gerät die Regel für das Verschieben angewandt wird (**Unbekannt**, **x86**, **AMD64**, **IA64**). Standardmäßig ist in dieser Liste keine Variante ausgewählt, die Architektur des Betriebssystems ist nicht angegeben.

- Service Pack-Version des Betriebssystems

  In diesem Feld können Sie die 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.

- Build-Version des Betriebssystems

Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

Versionsnummer des Betriebssystems. Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Versionsnummer haben muss. Sie können auch eine Suche nach allen Versionsnummern mit Ausnahme der angegebenen anpassen.

- Release-ID des Betriebssystems

  Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

  Release-Identifikator (ID) des Betriebssystems Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Release-ID haben muss. Sie können auch eine Suche nach allen Release-ID-Nummern mit Ausnahme der angegebenen anpassen.

Gerätestatus

Im Abschnitt **Gerätestatus** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Beschreibung des Gerätestatus des verwalteten Programms anpassen:

- Gerätestatus

  In dieser Dropdown-Liste können Sie einen Gerätestatus auswählen: *OK*, *Kritisch* oder *Warnung*.

- Beschreibung des Gerätestatus

  In diesem Feld können Sie die Kontrollkästchen für jene Bedingungen aktivieren, auf deren Basis einem Gerät eine der folgenden Statusvarianten zugewiesen werden soll: *OK, Kritisch* oder *Warnung*.

- Vom Programm bestimmter Gerätestatus

  In dieser Dropdown-Liste können Sie den Wert für den Status des Echtzeitschutzes auswählen. Geräte mit dem angegebenen Echtzeitschutz-Status werden in die Auswahl aufgenommen.

Schutzkomponenten

Im Abschnitt **Schutzkomponenten** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand des Schutzstatus anpassen:

- Veröffentlichung der Datenbanken

Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach dem Veröffentlichungsdatum der Antiviren-Datenbanken. In den Eingabefeldern können Sie den Zeitraum festlegen, anhand dessen die Suche ausgeführt werden soll.

Diese Option ist standardmäßig deaktiviert.

- Letzte Virensuche

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach dem Zeitpunkt der letzten Untersuchung auf Viren. In den Eingabefeldern können Sie den Zeitraum festlegen, in dem die Untersuchung auf Viren zum letzten Mal erfolgte.

  Diese Option ist standardmäßig deaktiviert.

- Gesamtzahl der gefundenen Bedrohungen

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach der Anzahl der gefundenen Viren. In den Eingabefeldern können Sie den unteren und oberen Wert für die Anzahl der gefundenen Viren festlegen.

  Diese Option ist standardmäßig deaktiviert.

Programm-Registry

Auf der Registerkarte **Programm-Registry** können Sie die Kriterien für die Aufnahme von Geräten anhand von installierten Programmen anpassen:

- Programmname

  In dieser Dropdown-Liste können Sie 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.

- Programm-Status

  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.

Hardware-Inventur

Im Abschnitt **Hardware-Inventur** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der auf ihnen installierten Hardware anpassen:

- Gerät

  In dieser Dropdown-Liste können Sie einen Einheitentyp auswählen. Alle Geräte mit dieser Einheit werden in die Suchergebnisse aufgenommen.

  Im Feld wird die Volltextsuche unterstützt.

- Hersteller

  In dieser Dropdown-Liste können Sie den Namen eines Herstellers der Einheit auswählen. Alle Geräte mit dieser Einheit werden in die Suchergebnisse aufgenommen.

  Im Feld wird die Volltextsuche unterstützt.

- Gerätename

  Ein Gerät mit dem angegebenen Namen wird in die Auswahl aufgenommen.

- **Beschreibung**

  Beschreibung des Geräts oder der Hardware. Geräte mit der in diesem Feld angegebenen Beschreibung werden in die Auswahl aufgenommen.

  Eine Beschreibung in beliebiger Form kann im Fenster Geräteeigenschaften eingegeben werden. Im Feld wird die Volltextsuche unterstützt.

- **Gerätehersteller**

  Bezeichnung des Geräteherstellers. Geräte, die vom angegebenen Hersteller produziert wurden, werden in die Auswahl aufgenommen.

  Der Name des Herstellers kann im Fenster Geräteeigenschaften eingegeben werden.

- **Seriennummer**

  Hardware mit in diesem Feld angegebener Seriennummer wird in die Auswahl aufgenommen.

- **Inventarnummer**

  Hardware mit in diesem Feld angegebener Inventarnummer wird in die Auswahl aufgenommen.

- **Benutzer**

  Hardware des in diesem Feld angegebenen Benutzers wird in die Auswahl aufgenommen.

- **Ort**

  Standort des Geräts bzw. der Hardware (z. B. im Büro oder in der Filiale). Computer oder andere Geräte am in diesem Feld angegebenen Ort werden in die Auswahl aufgenommen.

  Der Ort der Hardware kann in beliebiger Form im Hardware-Eigenschaftenfenster eingegeben werden.

- **Prozessorfrequenz in MHz**

  Frequenzbereich des Prozessors. Geräte mit Prozessoren, die dem Frequenzbereich in den Eingabefeldern entsprechen (inklusiv), werden in die Auswahl aufgenommen.

- **Virtuelle Prozessorkerne**

  Bereich der Anzahl von virtuellen Cores des Prozessors. Geräte mit Prozessoren, die dem Bereich in den Eingabefeldern entsprechen (inklusiv), werden in die Auswahl aufgenommen.

- **Größe der Festplatte (GB)**

  Bereich der Festplattengröße des Geräts. Geräte mit Festplatten, die dem Bereich in den Eingabefeldern entsprechen (inklusiv), werden in die Auswahl aufgenommen.

- Speichergröße (MB)

  Größenbereich des Arbeitsspeichers des Geräts. Geräte mit einem Arbeitsspeicher, der dem Bereich in den Eingabefeldern entspricht (inklusiv), werden in die Auswahl aufgenommen.

Virtuelle Maschinen

Auf der Registerkarte **Virtuelle Maschinen** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anpassen, je nachdem, ob diese Geräte virtuelle Maschinen sind oder zur Virtual Desktop Infrastructure (VDI) gehören:

- Ist eine virtuelle Maschine

  Sie können in der Dropdown-Liste folgende Elemente wählen:
  - **Unwichtig**.
  - **Nein**. Die gesuchten Geräte dürfen keine virtuellen Maschinen sein.
  - **Ja**. Die gesuchten Geräte müssen virtuelle Maschinen sein.

- Typ der virtuellen Maschine

  In der Dropdown-Liste können Sie den Hersteller der virtuellen Maschine auswählen.

  Die Dropdown-Liste ist verfügbar, wenn die Werte **Ja** oder **Unwichtig** in der Dropdown-Liste **Ist eine virtuelle Maschine** gewählt wurden.

- Teil einer Virtual Desktop Infrastructure (VDI)

  Sie können in der Dropdown-Liste folgende Elemente wählen:
  - **Unwichtig**.
  - **Nein**. Die gesuchten Geräte dürfen kein Teil der Virtual Desktop Infrastructure (VDI) sein.
  - **Ja**. Die gesuchten Geräte müssen Teil der Virtual Desktop Infrastructure (VDI) sein.

Benutzer

Auf der Registerkarte **Benutzer** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Benutzerkonten anpassen, die sich am Betriebssystem angemeldet haben.

- Letzter am System angemeldeter Benutzer

  Ist diese Option aktiviert, können Sie durch Klicken auf die Schaltfläche **Durchsuchen** ein Benutzerkonto auswählen. In die Suchergebnisse werden Geräte aufgenommen, auf denen sich der angegebene Benutzer als Letzter angemeldet hat.

- Benutzer, der sich mindestens einmal am System angemeldet hat

Ist diese Option aktiviert, können Sie durch Klicken auf die Schaltfläche **Durchsuchen** ein Benutzerkonto auswählen. In die Suchergebnisse werden Geräte aufgenommen, auf denen sich der angegebene Benutzer mindestens einmal im System angemeldet hat.

Statusbeeinflussende Probleme in verwalteten Programmen

Im Abschnitt **Statusbeeinflussende Probleme in verwalteten Programmen** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Liste von möglichen von einem verwalteten Programm gefundenen Problemen anpassen. Wenn zumindest ein ausgewähltes Problem auf einem Gerät existiert, wird das Gerät in die Auswahl aufgenommen. Wenn Sie ein Problem auswählen, das für mehrere Programme aufgelistet ist, haben Sie die Möglichkeit, dieses Problem in allen Listen automatisch auszuwählen.

Beschreibung des Gerätestatus

Sie können die Kontrollkästchen für die Beschreibung der Status der verwalteten Programme aktivieren, bei deren Empfang die Geräte in die Auswahl aufgenommen werden. Wenn Sie einen Status auswählen, der für mehrere Programme aufgelistet ist, haben Sie die Möglichkeit, diesen Status in allen Listen automatisch auszuwählen.

Status der Komponenten in verwalteten Programmen

Im Abschnitt **Status der Komponenten in verwalteten Programmen** können Sie Kriterien für die Aufnahme von Geräten in eine Auswahl anhand der Status der Komponenten der verwalteten Programme anpassen:

- Status des Schutzes vor Datenverlust

  Suche nach Geräten anhand des Status des "Schutzes vor Datenverlust" (*Keine Gerätedaten, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

- Status des Schutzes der Server für die Zusammenarbeit

  Suche nach Geräten anhand des Status der Komponente "Schutz der Serverzusammenarbeit" (*Keine Gerätedaten*, *Beendet*, *Wird gestartet, Angehalten*, *Wird ausgeführt*, *Fehlgeschlagen*).

- Status des Antiviren-Schutzes von Mail-Servern

  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*).

Programmkomponenten

Dieser Abschnitt enthält die Liste der Komponenten jener Anwendungen, in denen entsprechende Verwaltungs-Plug-ins in der Verwaltungskonsole installiert sind.

Im Abschnitt **Programmkomponenten** können Sie Kriterien für die Aufnahme von Geräten in eine Auswahl anhand der Status und Versionsnummern der Komponenten festlegen, die sich auf die ausgewählte Anwendung beziehen:

- **Status**

  Suche nach Geräten anhand des Status der Komponente, der von einer Anwendung an den Administrationsserver gesendet wurde. Sie können einen der folgenden Status auswählen: *Keine Daten des Geräts verfügbar*, *Beendet*, *Wird gestartet*, *Angehalten*, *Wird ausgeführt*, *Fehler* oder *Nicht installiert*. Wenn die ausgewählte Komponente der auf einem verwalteten Gerät installierten Anwendung den angegebenen Status aufweist, wird das Gerät bei der Geräteauswahl berücksichtigt.

  Von Anwendungen gesendete Status:

  - *Start*—Die Komponente wird gerade initialisiert.
  - *Wird ausgeführt*–Die Komponente ist aktiviert und funktioniert ordnungsgemäß.
  - *Angehalten*–Die Komponente wird angehalten, z. B. nachdem der Benutzer den Schutz in der verwalteten Anwendung angehalten hat.
  - *Fehler*–Während des Betriebs der Komponente ist ein Fehler aufgetreten.
  - *Beendet*–Die Komponente ist deaktiviert und funktioniert momentan nicht.
  - *Nicht installiert*–Der Benutzer hat die Komponente während der Konfiguration der benutzerdefinierten Installation der Anwendung nicht für die Installation ausgewählt.

  Im Gegensatz zu anderen Status wird der Status *Keine Daten des Geräts verfügbar* nicht von Programmen versendet. Diese Option zeigt, dass die Programme über keine Informationen über den ausgewählten Status der Komponente aufweisen. Dies kann beispielsweise der Fall sein, wenn die ausgewählte Komponente zu keiner der auf dem Gerät installierten Anwendungen gehört oder wenn das Gerät ausgeschaltet ist.

- **Version**

  Suche nach Geräten anhand der Versionsnummer der in der Liste ausgewählten Komponente. Sie können eine Versionsnummer eingeben, beispielsweise `3.4.1.0`, und dann festlegen, ob die ausgewählte Komponente eine gleich, frühere oder spätere Version aufweisen muss. Sie können auch eine Suche nach allen Versionen mit Ausnahme der angegebenen anpassen.

API-Referenzhandbuch

Dieses Kaspersky Security Center OpenAPI-Referenzhandbuch soll Sie bei den folgenden Aufgaben unterstützen:

- Automatisierung und Individualisierung. Sie können dadurch Aufgaben automatisieren, die nicht manuell ausgeführt werden sollen. Beispielsweise können Sie Kaspersky Security Center OpenAPI dazu verwenden, Scripte zu erstellen und auszuführen, die das Entwickeln und Pflegen einer Struktur von Administrationsgruppen vereinfachen.

- Individuelle Entwicklung. Mit OpenAPI können Sie eine Client-Anwendung entwickeln.

Sie können das Suchfeld auf der rechten Seite des Bildschirms verwenden, um im OpenAPI-Referenzhandbuch die von Ihnen benötigten Informationen zu finden.

OPENAPI-REFERENZHANDBUCH

Skriptbeispiele

Das OpenAPI-Referenzhandbuch enthält Beispiele für die in der folgenden Tabelle aufgeführten Python-Skripts. Diese Beispiele zeigen, wie Sie OpenAPI-Methoden aufrufen und verschiedene Aufgaben zum Schutz Ihres Netzwerks automatisch ausführen können, z. B. das Erstellen einer "primär/sekundär"-Hierarchie, das Ausführen von Aufgaben in Kaspersky Security Center oder das Zuweisen von Verteilungspunkten. Sie können die Beispiele unverändert ausführen oder Ihre eigenen Skripts basierend auf den Beispielen erstellen.

Um die OpenAPI-Methoden aufzurufen und Skripte auszuführen:

1. Laden Sie das Archiv KlAkOAPI.tar.gz herunter. Dieses Archiv enthält das KlAkOAPI-Paket und Beispiele (Sie können diese aus dem Archiv oder dem OpenAPI-Referenzhandbuch kopieren).

2. Installieren Sie das Paket KlAkOAPI aus dem Archiv KlAkOAPI.tar.gz auf einem Gerät mit installiertem Administrationsserver.

   Sie können nur auf Geräten, auf denen der Administrationsserver und das Paket KlAkOAPI installiert sind, OpenAPI-Methoden aufrufen, Beispiele ausführen und eigene Skripte ausführen.

Benutzerszenarien und Beispiele für entsprechende Kaspersky Security Center OpenAPI-Methoden

Beispiel	Ziel des Beispiels	Szenario
Loggen von KlAkParams	Unter Verwendung der `KlAkParams`-Datenstruktur können Sie Daten extrahieren und verarbeiten. Das ist ein Beispiel für die Arbeit mit dieser Datenstruktur. Die Ausgabe des Beispiels kann auf verschiedene Weisen präsentiert werden. Sie können die Daten erhalten, um eine HTTP-Methode zu versenden, oder um Sie in Ihrem Code zu verwenden.	Überwachung und Berichterstattung
"Primär/Sekundär"-Hierarchie erstellen und löschen	Sie können einen sekundären Administrationsserver hinzufügen und so eine Hierarchie vom Typ "primär/sekundär" festlegen. Alternativ können Sie den sekundären Administrationsserver von der Hierarchie trennen.	Erstellen einer Hierarchie von Administrationsservern, Hinzufügen eines sekundären Administrationsservers und Löschen einer

		Hierarchie von Administrationsservern
Netzwerklisten-Dateien mittels Verbindungs-Gateway auf den angegebenen Host herunterladen	Unter Verwendung eines Verbindungs-Gateways können Sie sich mit dem Administrationsagenten des benötigten Geräts verbinden und anschließend die Datei mit der Netzwerkliste auf Ihr Gerät herunterladen.	Verteilungspunkte und Verbindungs-Gateways anpassen
Einen Lizenzschlüssel, der sich in der Datenverwaltung des primären Administrationsservers befindet, auf sekundären Administrationsservern installieren	Sie können sich mit dem primären Administrationsserver verbinden, von ihm einen erforderlichen Lizenzschlüssel herunterladen, und diesen Schlüssel an alle in der Hierarchie enthaltenen sekundären Administrationsserver weiterleiten.	Lizenzierung der verwalteten Programme
Erstellen eines Berichts über gültige Benutzerberechtigungen	Sie können verschiedene Berichte erstellen. Unter anderem können Sie den Bericht über gültige Benutzerberechtigungen unter Verwendung dieses Beispiels erstellen. Dieser Bericht gibt die Berechtigungen eines Benutzers in Abhängigkeit seiner oder ihrer Gruppe und Rolle an. Sie können den Bericht in den folgenden Formaten herunterladen: HTML, PDF oder Excel.	Bericht erstellen und anzeigen
Starten der Aufgabe für ein Gerät	Unter Verwendung eines Verbindungs-Gateways können Sie sich mit dem Administrationsagenten des benötigten Geräts verbinden und anschließend die notwendige Aufgabe starten.	Manuelles Starten einer Aufgabe
Registrieren von Verteilungspunkten für Geräte in einer Gruppe	Sie können verwalteten Geräten die Rolle eines Verteilungspunkts (früher bekannt als "Update-Agent") zuweisen.	Kaspersky-Datenbanken und -Anwendungen aktualisieren
Alle Gruppen durchzählen	Sie können mit Administrationsgruppen verschiedene Aktionen ausführen. Das Beispiel zeigt Folgendes: • Eine ID der Root-Gruppe der "Verwalteten Geräte" abrufen • Durch die Gruppenhierarchie bewegen • Die vollständige, erweiterte Gruppenhierarchie, einschließlich ihrer Namen und Vierschachtelungen abrufen	Konfigurieren des Administrationsservers
Aufgaben durchzählen, Aufgabenstatistiken abfragen und Aufgaben ausführen	Die folgenden Informationen können Sie abfragen: • Verlauf des Aufgabenprozesses • Aktueller Aufgabenstatus • Anzahl der Aufgaben mir unterschiedlichen Statuswerten	Aufgabenausführung überwachen

	Sie können auch eine Aufgabe starten. Standardmäßig startet das Beispiel eine Aufgabe, nachdem es Statistiken ausgegeben hat.	
Eine Aufgabe erstellen und ausführen	Sie können eine Aufgabe erstellen. Geben Sie in dem Beispiel die folgenden Aufgabenparameter an: • Typ • Art der Ausführung • Name • Gerätegruppe, auf welche die Aufgabe angewendet wird Standardmäßig erstellt das Beispiel eine Aufgabe des Typs "Nachricht anzeigen". Sie können diese Aufgabe für alle verwalteten Geräte des Administrationsservers ausführen. Bei Bedarf können Sie eigene Aufgabenparameter angeben.	Erstellen einer Aufgabe
Lizenzschlüssel durchzählen	Sie können eine Liste mit allen aktiven Lizenzschlüsseln für Kaspersky-Programme abrufen, die auf den verwalteten Geräten des Administrationsservers installiert sind. Die Liste enthält detaillierte Informationen über jeden Lizenzschlüssel, darunter Name, Typ oder Ablaufdatum.	Informationen zu verwendeten Lizenzschlüsseln anzeigen
Einen internen Benutzer erstellen und auffinden	Sie können ein Benutzerkonto zur weiteren Bearbeitung erstellen.	Auswählen des Benutzerkontos für den Start des Administrationsservers
Eine benutzerdefinierte Kategorie erstellen	Sie können eine Programmkategorie mit den benötigten Parametern erstellen.	Manuell zu erweiternde Programmkategorie erstellen
Benutzer mittels SrvView durchzählen	Sie können die Klasse SrvView verwenden, um detaillierte Informationen vom Administrationsserver abzufragen. Unter Verwendung dieses Beispiels können Sie unter anderem eine Liste der Benutzer abrufen.	Benutzerkonten verwalten

Anwendungen, die über OpenAPI mit Kaspersky Security Center interagieren

Einige Anwendungen können über OpenAPI mit Kaspersky Security Center interagieren. Zu solchen Anwendungen gehören beispielsweise Kaspersky Anti Targeted Attack Platform und Kaspersky Security for Virtualization. Dies kann auch ein von Ihnen entwickelte benutzerdefinierte Client-Anwendung auf Basis von OpenAPI sein.

Anwendungen, die über OpenAPI mit Kaspersky Security Center interagieren, verbinden sich mit dem Administrationsserver. Wenn Sie für die Verbindung mit dem Administrationsserver eine Allow-Liste mit IP-Adressen konfiguriert haben, fügen Sie die IP-Adressen von den Geräten hinzu, auf denen Anwendungen laufen, die Kaspersky Security Center OpenAPI verwenden. Weitere Informationen darüber, ob die von Ihnen verwendete Anwendung durch OpenAPI unterstützt wird, entnehmen Sie der Hilfe der entsprechenden Anwendung.

Integration von Kaspersky Security Center Web Console und anderen Kaspersky-Lösungen

Dieser Abschnitt beschreibt, wie Sie den Zugriff von Kaspersky Security Center Web Console auf andere Kaspersky-Programme, wie Kaspersky Endpoint Detection and Response Optimum und Kaspersky Managed Detection and Response, konfigurieren.

Anpassen des Zugriffs auf die KATA/KEDR Web Console

Kaspersky Anti Targeted Attack (KATA) und Kaspersky Endpoint Detection and Response (KEDR) sind zwei funktionale Blöcke der Kaspersky Anti Targeted Attack Platform. Sie können diese funktionalen Blöcke über die Web Console für Kaspersky Anti Targeted Attack Platform (KATA/KEDR Web Console) verwalten. Wenn Sie Kaspersky Security Center 14 Web Console und die KATA / KEDR Web Console verwenden, können Sie den Zugriff auf die KATA/KEDR Web Console direkt über die Benutzeroberfläche von Kaspersky Security Center 14 Web Console verwalten.

Um den Zugriff auf die KATA/KEDR Web Console zu konfigurieren:

1. Klicken Sie oben im Programmhauptfenster auf **Konsolen-Einstellungen**.
2. Wählen Sie im Dropdown-Menü den Punkt **Integration** aus.

   Das Fenster "Konsolen-Einstellungen" wird geöffnet.
3. Geben Sie auf der Registerkarte **Integration** im Feld **URL der Web Console von KATA/KEDR** die URL der KATA/KEDR Web Console ein.
4. Klicken Sie auf die Schaltfläche **Speichern**.

Die Dropdown-Liste **Integrationen** wird dem Hauptfenster der Anwendung hinzugefügt. Über dieses Menü können Sie die KATA/KEDR Web Console öffnen. Nach dem Klicken auf **Advanced Cybersecurity**, öffnet sich in Ihrem Browser eine neue Registerkarte mit der von Ihnen angegebenen URL.

Eine Hintergrundverbindung herstellen

Zur Konfiguration der Interaktion zwischen Kaspersky Security Center und einem anderen Programm oder einer Lösung von Kaspersky wie beispielsweise Kaspersky Managed Detection and Response (auch MDR genannt) müssen Sie eine Hintergrundverbindung zwischen Kaspersky Security Center Web Console und dem Administrationsserver herstellen. Sie können diese Verbindung nur dann herstellen, wenn Ihr Benutzerkonto die Berechtigung "Objekt-ACL ändern" im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** hat.

Sie können die Interaktion nur zwischen Kaspersky Managed Detection and Response und der Windows-basierten Version von Kaspersky Security Center konfigurieren.

So stellen Sie eine Hintergrundverbindung her:

1. Wählen Sie in der Dropdown-Liste **Konsolen-Einstellungen** die Option **Integration**.

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

2. Wählen Sie die Registerkarte **Integration** aus.

3. Wählen Sie auf der Registerkarte **Integration** den Abschnitt **Integration** aus.

4. Stellen Sie den Umschalter zum Herstellen einer Background-Verbindung auf die Position: **Background-Verbindung für die Integration herstellen AKTIVIERT**.

5. Klicken Sie im geöffneten Abschnitt **Der Dienst zum Herstellen einer Background-Verbindung wird auf dem Server der Kaspersky Security Center Web Console gestartet** auf die Schaltfläche **Uhrzeit der Verschlüsselung**.

Die Background-Verbindung zwischen Kaspersky Security Center Web Console und dem Administrationsserver ist hergestellt. Der Administrationsserver erstellt für die Background-Verbindung ein Benutzerkonto, welches als Dienstkonto verwendet wird, um die Interaktion zwischen Kaspersky Security Center und einer anderen Kaspersky-Anwendung aufrecht zu erhalten. Der Name des Dienstkontos enthält den Präfix "NWCSvcUser". Aus Sicherheitsgründen ändert der Administrationsserver das Kennwort des Dienstkontos automatisch alle 30 Tage. Das Dienstkonto kann nicht manuell gelöscht werden. Der Administrationsserver löscht dieses Konto automatisch, wenn Sie die Cross-Service-Verbindung deaktivieren. Der Administrationsserver erstellt ein Benutzerkonto für jede Kaspersky Security Center 14 Web Console und Verwaltungskonsole und weist all diese Dienstkonten der Sicherheitsgruppe mit dem Namen "ServiceNwcGroup" zu. Der Administrationsserver erstellt diese Sicherheitsgruppe automatisch während der Installation von Kaspersky Security Center. Diese Sicherheitsgruppe kann nicht manuell gelöscht werden.

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 Linux noch in den anderen Informationsquellen zu Kaspersky Security Center Linux keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support. Die Mitarbeiter des Technischen Supports beantworten alle Fragen zur Installation und Verwendung von Kaspersky Security Center Linux.

Kaspersky bietet die Unterstützung für Kaspersky Security Center Linux im Rahmen dessen Lebenszyklus' an (siehe Seite über den 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 per Telefon

Unseren Technischen Support können Sie aus den meisten Regionen telefonisch erreichen. Informationen darüber, wie Sie in Ihrer Region technischen Support erhalten, sowie Kontaktinformationen des Technischen Supports finden Sie auf der Website des Kundendienstes von Kaspersky.

Bitte beachten Sie die Support-Richtlinien, bevor Sie sich an den Technischen Support wenden.

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.

Informationsquellen über das Programm

Seite von Kaspersky Security Center auf der Website von Kaspersky

Auf der Seite über Kaspersky Security Center auf der Kaspersky Website finden Sie allgemeine Informationen über die Anwendung, ihre Funktionen und Besonderheiten.

Seite von Kaspersky Security Center in der Wissensdatenbank

Die *Wissensdatenbank* ist ein Abschnitt der Website des Technischen Supports von Kaspersky.

Auf der Seite von Kaspersky Security Center Linux in der Wissensdatenbank finden Sie Artikel mit nützlichen Informationen, Tipps und Antworten auf häufige Fragen zum Kauf, zur Installation und zur Nutzung des Programms.

Neben Fragen zu Kaspersky Security Center 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 sie 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 Linux hat eine Reihe von Einschränkungen, die für die Verwendung des Programms nicht kritisch sind:

- In der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und der Aufgabe *Download von Updates in die Datenverwaltung der Verteilungspunkte* funktioniert die Benutzerauthentifizierung nicht, wenn Sie einen kennwortgeschützten lokalen Ordner oder Netzwerkordner als Update-Quelle auswählen. Um dieses Problem zu beheben, stellen Sie zuerst den kennwortgeschützten Ordner bereit und geben Sie dann die erforderlichen Anmeldedaten an, z. B. über das Betriebssystem. Danach können Sie diesen Ordner als Update-Quelle in einer Aufgabe für Update-Downloads auswählen. Für Kaspersky Security Center müssen Sie keine Anmeldedaten eingeben.

- Die Aufgabe *Administrationsserver ändern* wird nicht automatisch gestartet, nachdem Sie die Option **Sofort** im Aufgabenplan ausgewählt und die Änderungen gespeichert haben.

- Wenn Sie in den Eigenschaften des Administrationsservers Proxyserver-Einstellungen angeben und anschließend in der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* die Option **Proxyserver nicht verwenden** aktivieren, wird diese Option ignoriert und eine Verbindung über einen Proxyserver hergestellt.

- Wenn Sie Kaspersky Security Center 14 Web Console in verschiedenen Browsern öffnen und im Eigenschaftenfenster des Administrationsservers die Datei mit dem Zertifikat des Administrationsservers herunterladen, haben die Dateien unterschiedliche Namen.

- Wenn Sie ein Objekt aus der Datenverwaltung **BACKUP** (**VORGÄNGE → DATENVERWALTUNG → BACKUP**) wiederherstellen oder an Kaspersky senden möchten, tritt ein Fehler auf.

- Die Einstellungen einer übergeordneten Richtlinie von Kaspersky Endpoint Security für Linux werden an untergeordnete Richtlinien vererbt, aber nicht gesperrt.

- Die von einem verwalteten Gerät an den Administrationsserver gesendeten Hardware-Informationen sind möglicherweise nicht vollständig. Einige Hardware-Elemente werden möglicherweise nicht angegeben.

- Eine Programmkategorie, die Sie in der Richtlinie für Kaspersky Endpoint Security für Linux zur Programmkontrolle hinzugefügt haben, kann gelöscht werden.

- Ein verwaltetes Gerät, dass über mehr als einen Netzwerkadapter verfügt, übermittelt an den Administrationsserver die MAC-Adressinformationen von dem Netzwerkadapter, der nicht zum Herstellen der Verbindung mit dem Administrationsserver verwendet wird.

- Wenn Sie in einer Antwortdatei für die Installation von Kaspersky Security Center 14 Web Console in den Parametern webConsoleAccount und managementServiceAccount benutzerdefinierte Benutzerkonten angeben und diese Konten zu verschiedenen Sicherheitsgruppen gehören, funktioniert Kaspersky Security Center 14 Web Console nach der Installation nicht.

- In der Astra Linux 64-Bit-Edition kann das Paket "klnagent-astra" nicht mit dem Paket "klnagent64_14" aktualisiert werden: Das alte Paket "klnagent64-astra" wird entfernt und das neue Paket "klnagent64" wird anstelle des Upgrades installiert. Es wird daher das neue Symbol für das Gerät mit dem Paket "klnagent64_14" hinzugefügt. Sie können das alte Symbol für dieses Gerät entfernen.

Glossar

Administrationsagent

Eine Komponente von Kaspersky Security Center, mit deren Hilfe die Interaktion zwischen dem Administrationsserver und den Programmen von Kaspersky ermöglicht wird, die auf einem bestimmten Netzwerk-Knoten (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, die Informationen über alle Programme von Kaspersky, die innerhalb des Unternehmensnetzwerks installiert sind, zentral speichert. Sie kann auch zur Verwaltung dieser Programme verwendet werden.

Administrationsserver-Client (Client-Gerät)

Gerät, Server oder Workstation, auf welchem bzw. welcher der Administrationsagent installiert ist und verwaltete Programme von Kaspersky ausgeführt werden.

Administrator des Anbieters

Mitarbeiter eines Anbieters von Antiviren-Schutz. Dieser Administrator führt Installations- und Verwaltungsaufträge für Antiviren-Schutzsysteme auf der Grundlage von Antiviren-Produkten von Kaspersky durch und bietet darüber hinaus technischen Support für Kunden.

Administrator-Arbeitsplatz

Ein Gerät, auf dem Sie Kaspersky Security Center 14 Web Console öffnen. Diese Komponente stellt eine Verwaltungsschnittstelle von Kaspersky Security Center bereit.

Der Administrator-Arbeitsplatz wird zur Konfiguration und Verwaltung der Serverseite von Kaspersky Security Center verwendet. Mithilfe des Administrator-Arbeitsplatzes erstellt und verwaltet der Administrator ein zentralisierten Antiviren-Schutzsystem für ein Unternehmens-LAN auf der Grundlage von Programmen von Kaspersky.

Administratorberechtigungen

Stufe der Benutzerberechtigungen und Rechte, die für die Verwaltung von Exchange-Objekten innerhalb einer Exchange-Organisation erforderlich sind.

Aktiver Schlüssel

Ein Schlüssel, der momentan vom Programm verwendet wird.

Anbieter von Antiviren-Schutz

Ein Unternehmen, das für ein Kundenunternehmen einen Antiviren-Schutz auf der Grundlage von Lösungen von Kaspersky bereitstellt.

Antiviren-Datenbanken

Datenbanken, die Informationen über diejenigen Bedrohungen der Computersicherheit enthalten, die Kaspersky zum Zeitpunkt des Erscheinens der Antiviren-Datenbanken bekannt sind. Durch die Eintragungen in den Antiviren-Datenbanken kann in den untersuchten Objekten bösartiger Code erkannt werden. Antiviren-Datenbanken werden von den Experten von Kaspersky erstellt und stündlich aktualisiert.

App Store

Komponente von Kaspersky Security Center. Der App Store wird zur Installation von Apps auf Android-Geräten von Benutzern verwendet. Der App Store erlaubt Ihnen, die APK-Dateien von Apps und Links zu Apps in Google Play zu veröffentlichen.

Aufgabe

Funktionen, die 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.

Backup-Ordner

Spezieller Ordner zum Speichern von Kopien der Daten des Administrationsservers, die mithilfe des Backup-Tools erstellt werden.

Broadcast-Domäne

Logischer Bereich eines Netzwerks, in dem alle Knoten mithilfe eines Broadcast-Kanals auf OSI-Ebene (Open Systems Interconnection Basic Reference Model) Daten austauschen können.

Client-Administrator

Mitarbeiter eines Kundenunternehmens, der für die Überwachung des Antiviren-Schutzstatus verantwortlich ist.

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. Dort werden Informationen über in Kaspersky Security Center Linux auftretende Ereignisse gespeichert.

Ereignispriorität

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 Signifikanz aufweisen.

Gerätebesitzer

Der Gerätebesitzer ist ein Benutzer, an den sich der Administrator wenden kann, wenn Bedarf zur Durchführung bestimmter Operationen auf einem Gerät besteht.

Geteiltes Zertifikat

Ein Zertifikat, das zur Identifizierung des mobilen Geräts des Benutzers dient.

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.

Inkompatibles Programm

Ein Antiviren-Programm eines Drittanbieters oder ein Kaspersky-Programm, das die Verwaltung über Kaspersky Security Center Linux nicht unterstützt.

Installationspaket

Satz von Dateien, der für die Remote-Installation eines Kaspersky-Programms mithilfe des Remote-Verwaltungssystems von Kaspersky Security Center erstellt wurde. Das Installationspaket enthält eine Reihe von Einstellungen, die für die Installation und Inbetriebnahme der Anwendung nach der Installation benötigt werden. Die Einstellungen entsprechen der Standardkonfiguration der Anwendung. Das Installationspaket wird mithilfe von Dateien mit der Erweiterung .kpd und .kud erstellt, die im Lieferumfang der Anwendung enthalten sind.

Interne Benutzer

Die Benutzerkonten der internen Benutzer werden für die Arbeit mit den virtuellen Administrationsservern verwendet. Innerhalb der Funktionen von Kaspersky Security Center verfügen die internen Benutzer über die Berechtigungen tatsächlicher Benutzer.

Benutzerkonten der internen Benutzer werden nur innerhalb von Kaspersky Security Center erstellt und verwendet. Informationen über die internen Benutzer werden nicht auf das Betriebssystem übertragen. Die Authentifizierung der internen Benutzer erfolgt über Kaspersky Security Center.

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 (Private KSN)

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 Benutzergeräte 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 Administrator

Person, die Programmvorgänge über das zentralisierte Remote-Verwaltungssystem Kaspersky Security Center verwaltet.

Kaspersky Security Center Operator

Benutzer, der den Status und Betrieb eines Schutzsystems überwacht, das mithilfe von Kaspersky Security Center verwaltet wird.

Kaspersky Security Center System Health Validator (SHV)

Komponente von Kaspersky Security Center, die zur Überprüfung der Einsatzfähigkeit des Betriebssystems im Fall von gleichzeitigem Betrieb von Kaspersky Security Center und Microsoft NAP dient.

Kaspersky Security Center Webserver

Komponente von Kaspersky Security Center, die gemeinsam mit dem Administrationsserver installiert wird. Der Webserver dient dazu, autonome Installationspakete, iOS MDM-Profile sowie Dateien aus einem freigegebenen Ordner im Netzwerk zu übertragen.

Kaspersky-Update-Server

HTTP(S)-Server bei Kaspersky, von denen Programme von Kaspersky Updates für Datenbanken und Programm-Module herunterladen.

Konfigurationsprofil

Richtlinie, die eine Zusammenstellung von Einstellungen und Einschränkungen für ein mobiles iOS MDM-Gerät enthält.

Lizenzierte Programmgruppe

Gruppe von Programmen, die auf der Grundlage von Kriterien erstellt wird, die vom Administrator festgelegt werden (beispielsweise nach Hersteller), für die Statistiken zu den Installationen auf Client-Geräten geführt werden.

Lokale Aufgabe

Aufgabe, die auf einem einzelnen Client-Computer definiert wurde und ausgeführt wird.

Lokale Installation

Installation einer Sicherheitsanwendung auf einem Gerät in einem Unternehmensnetzwerk, die 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.

Manuelle Installation

Installation einer Sicherheitsanwendung aus dem Programmpaket auf einem Gerät im Unternehmensnetzwerk. Manuelle Installation erfordert die Einbeziehung eines Administrators oder anderen IT-Spezialisten. Im Normalfall wird eine manuelle Installation durchgeführt, wenn die Remote-Installation mit einem Fehler beendet wurde.

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.

Profil

Zusammenstellung von Einstellungen für mobile Geräte mit Exchange, die deren Verhalten definieren, wenn sie mit einem Microsoft Exchange-Server verbunden sind.

Programmeinstellungen

Programmeinstellungen, die für alle Aufgabentypen gleich sind und den Gesamtbetrieb des Programms regeln, zum Beispiel Leistungseinstellungen, Berichtseinstellungen und Backup-Einstellungen.

Provisioning-Profil

Zusammenstellung von Einstellungen für die Ausführung von Programmen auf mobilen iOS-Geräten. Ein Provisioning-Profil enthält Informationen zur Lizenz und ist mit einer bestimmten App verbunden.

Remote-Installation

Installation von Kaspersky-Apps über die von Kaspersky Security Center Linux 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.

Rollengruppe

Gruppe von Benutzern von mobilen Geräten mit Exchange ActiveSync, denen identische Administratorberechtigungen gewährt wurden.

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.

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, und Änderungen an der Programmarchitektur.

Verschieben der Daten des Administrationsservers ins Backup

Kopieren der Daten des Administrationsservers als Backup und zur anschließenden Wiederherstellung mithilfe des Backup-Tools. Das Tool kann Folgendes speichern:

- Datenbank des Administrationsservers (Richtlinien, Aufgaben, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse)
- Konfigurationsdaten über die Struktur von Administrationsgruppen und Client-Geräten
- Datenverwaltung der Installationsdateien zur Remote-Installation von Programmen (Inhalt der Ordner Pakete, Update-Deinstallation)
- Zertifikat des Administrationsservers

Verteilungspunkt

Computer, auf dem der Administrationsagent installiert ist und der zur Update-Verteilung, zur Remote-Installation von Programmen und zum Empfangen von Informationen über Computer in einer Administrationsgruppe und/oder Broadcasting-Domäne verwendet wird. Verteilungspunkte dienen dazu, die Belastung auf dem Administrationsserver während der Update-Verteilung zu verringern und den Netzwerkdatenverkehr zu optimieren. Verteilungspunkte können automatisch vom Administrationsserver oder manuell vom Administrator zugewiesen werden. Der Verteilungspunkt war in früheren Versionen als Update-Agent bekannt.

Verwaltete Geräte

Geräte in Unternehmensnetzwerken, die in einer Administrationsgruppe enthalten sind.

Verwaltungskonsole

Eine Komponente des Windows-basierten Kaspersky Security Center (auch "MMC-basierte Verwaltungskonsole" genannt). Diese Komponente stellt eine Benutzeroberfläche für die administrativen Dienste des Administrationsservers und des Administrationsagenten bereit. Die Verwaltungskonsole entspricht der Kaspersky Security Center 14 Web Console.

Virtueller Administrationsserver

Komponente von Kaspersky Security Center, die zur Verwaltung des Schutzsystems für das Netzwerk eines Kundenunternehmens dient.

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

- Ein virtueller Administrationsserver kann nur auf einem primären Administrationsserver erstellt werden.
- Ein virtueller Administrationsserver verwendet während seines Betriebs die Datenbank des primären Administrationsservers. Aufgaben zum Backup und zur Wiederherstellung von Dateien, sowie Aufgaben zur Suche nach Updates und Downloadaufgaben werden von einem virtuellen Administrationsserver nicht unterstützt.
- Für virtuelle Server können keine sekundären Administrationsserver angelegt werden (einschließlich virtueller Server).

Wiederherstellung

Wiederherstellung des ursprünglichen Objekts aus der Quarantäne oder dem Backup in seinem ursprünglichen Ordner, wo das Objekt gespeichert war, bevor es in die Quarantäne verschoben, desinfiziert oder gelöscht wurde, oder in einem benutzerdefinierten Ordner.

Wiederherstellung der Daten des Administrationsservers

Wiederherstellung der Daten des Administrationsservers aus den Informationen, die mithilfe des Backup-Tools im Backup gespeichert wurden. Das Tool kann Folgendes wiederherstellen:

- Datenbank des Administrationsservers (Richtlinien, Aufgaben, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse)
- Konfigurationsdaten über die Struktur von Administrationsgruppen und Client-Computern
- Datenverwaltung der Installationsdateien zur Remote-Installation von Programmen (Inhalt der Ordner Pakete, Update-Deinstallation)
- Zertifikat des Administrationsservers

Zentralisierte Programmverwaltung

Remote-Programmverwaltung mithilfe der Verwaltungsdienste, die in Kaspersky Security Center bereitgestellt werden.

Zertifikat des Administrationsservers

Das Zertifikat, das der Administrationsserver für folgende Zwecke verwendet:

- Authentifizierung des Administrationsservers beim Verbinden mit Kaspersky Security Center 14 Web Console
- Sichere Interaktion zwischen dem Administrationsserver und den Administrationsagenten auf verwalteten Geräten

- Authentifizierung von Administrationsservern beim Verbinden eines primären Administrationsservers mit einem sekundären Administrationsserver

Das Zertifikat wird bei der Installation des Administrationsservers automatisch erstellt und auf dem Administrationsserver gespeichert.

Zusätzlicher 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 sich im Installationsverzeichnis des Programms befindet.

Markenrechtliche Hinweise

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

Adobe, Acrobat, Flash, Shockwave und PostScript sind in den USA und/oder anderen Ländern eingetragene Markenzeichen oder Markenzeichen von Adobe.

AMD, AMD64 sind Warenzeichen oder eingetragene Marken von Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace sind Markenzeichen von Amazon.com, Inc. oder von verbundenen Unternehmen in den USA und/oder anderen Ländern.

Apache und Apache feather logo sind Markenzeichen von The Apache Software Foundation.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime und Touch ID sind in den USA und in anderen Ländern und Regionen eingetragene Markenzeichen von Apple Inc.

Die Bluetooth-Wortmarke und die Bluetooth-Logos sind Eigentum der Bluetooth SIG, Inc.

Ubuntu ist ein eingetragenes Markenzeichen von Canonical Ltd.

Cisco, Cisco Systems, IOS sind eingetragene 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 anderen Ländern eingetragen sein.

Corel ist eine Marke oder eingetragene Marke der Corel Corporation und/oder ihrer Tochtergesellschaften in Kanada, den USA und/oder anderen Ländern.

Dropbox ist ein Markenzeichen von Dropbox, Inc.

Firebird ist ein eingetragenes Warenzeichen der Firebird-Stiftung.

Foxit ist ein eingetragenes Markenzeichen der Foxit Corporation.

Das Logo FreeBSD ist ein eingetragenes Warenzeichen der Stiftung The FreeBSD.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Hangouts und YouTube sind Markenzeichen von Google LLC.

FusionCompute, FusionSphere sind in China und anderen Ländern eingetragene Markenzeichen von Huawei Technologies Co., Ltd.

Intel, Core und Xeon 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.

Micro Focus ist ein Markenzeichen oder eingetragenes Markenzeichen von Micro Focus (IP) Limited oder seinen Tochtergesellschaften in Großbritannien, den USA und anderen Ländern.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Server, Windows Phone, Windows Vista und Windows Azure sind Markenzeichen der Microsoft-Unternehmensgruppe.

Mozilla, Firefox, Thunderbird sind Markenzeichen der Mozilla Foundation.

Novell ist ein in den USA und anderen Ländern eingetragenes Markenzeichen von Novell Enterprises Inc.

Oracle, Java, JavaScript und TouchDown sind eingetragene Markenzeichen von Oracle und/oder von verbundenen Unternehmen.

Parallels und das Parallels-Logo sind Markenzeichen oder eingetragene Markenzeichen der Parallels International GmbH in Kanada, den Vereinigten Staaten und/oder anderswo.

Chef ist ein Markenzeichen oder eingetragenes Markenzeichen der Progress Software Corporation und/oder einer ihrer Tochtergesellschaften oder verbundenen Unternehmen in den USA und/oder anderen Ländern.

Puppet ist ein Markenzeichen oder eingetragenes Markenzeichen von Puppet, Inc.

Python ist ein Markenzeichen oder eingetragenes Markenzeichen der Python Software Foundation.

Red Hat, Ansible, CentOS, Fedora und Red Hat Enterprise Linux sind in den USA und in anderen Ländern Markenzeichen oder eingetragene Markenzeichen von Red Hat Inc oder seinen Tochtergesellschaften.

BlackBerry steht im Besitz von Research In Motion Limited ist in den USA eingetragen. Die Marke kann auch in anderen Ländern angemeldet oder eingetragen sein.

Debian ist ein eingetragenes Warenzeichen von Software in the Public Interest, Inc.

Splunk und SPL sind Markenzeichen und eingetragene Markenzeichen von Splunk Inc. in den USA und anderen Ländern.

SUSE ist ein in den USA und anderen Ländern eingetragenes Markenzeichen von SUSE LLC.

Das Markenzeichen Symbian ist Eigentum der Symbian Foundation Ltd.

OpenAPI ist ein Markenzeichen von The Linux Foundation.

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 Vereinigten Staaten und in anderen Ländern eingetragenes Markenzeichen. Die Nutzung wird durch die Firma X/Open Company Limited lizenziert.

Zabbix ist ein eingetragenes Markenzeichen von Zabbix SIA.