kaspersky

Kaspersky Endpoint Security für Linux

Inhalt

Über Kaspersky Endpoint Security 12.1 für Linux

Die App Kaspersky Endpoint Security 12.1 für Linux (im Folgenden auch Kaspersky Endpoint Security oder App genannt) schützt Geräte mit Linux®-Betriebssystemen vor verschiedenen Arten von Bedrohungen, Netzwerk- und betrügerischen Angriffen.

Mit der App lassen sich sowohl physische Geräte als auch virtuelle Maschinen schützen. Sie können die Kaspersky Endpoint Security als Teil der Lösung Kaspersky Security for Virtualization Light Agent für den Schutz virtueller Maschinen mit Linux-Gastbetriebssystemen verwenden.

Die Hauptfunktionen des Geräteschutzes und der Gerätekontrolle werden durch folgende Funktionskomponenten und Aufgaben der App gewährleistet:

- Der **Schutz vor bedrohlichen Dateien** verhindert eine Infektion des Dateisystem des Benutzergeräts. Die Komponente *Schutz vor bedrohlichen Dateien* startet automatisch beim Start von Kaspersky Endpoint Security und untersucht in Echtzeit alle Dateien, die geöffnet, gespeichert und ausgeführt werden.

  Sie können geschützte Geräte auch auf Befehl mithilfe der folgenden Untersuchungsaufgaben untersuchen:

  - **Schadsoftware-Untersuchung**. Die App untersucht Objekte des Dateisystems auf Schadsoftware, die sich auf den lokalen Laufwerken Ihres Geräts befinden, sowie alle eingebundenen und freigegebenen Ressourcen, auf die über SMB- und NFS-Protokolle zugegriffen wird. Mit dieser Aufgabe können Sie eine vollständige oder benutzerdefinierte Untersuchung des Geräts durchführen.

  - **Untersuchung wichtiger Bereiche**. Die App untersucht Bootsektoren, Autostart-Objekte sowie den Prozess- und den Kernelspeicher.

- **Untersuchung von Wechseldatenträgern**. Mit der Komponente *Untersuchung von Wechseldatenträgern* können Sie an das Gerät angeschlossene Wechseldatenträger in Echtzeit überwachen und den Wechseldatenträger und seine Bootsektoren auf Schadsoftware untersuchen. Kaspersky Endpoint Security kann die folgenden Wechseldatenträger untersuchen: CD-/DVD-Laufwerke, Blu-ray-Discs, Flash-Laufwerke (einschließlich USB-Modems), externe Festplatten und Disketten.

- **Untersuchung von Containern**. Mit der Komponente *Container-Überwachung* können Sie Namespaces und laufende Container in Echtzeit auf Schadsoftware untersuchen. Die Integration des Systems zur Verwaltung von Docker-Containern, der CRI-O-Umgebung und den Tools Podman und runc wird unterstützt. Mit der Aufgabe *Untersuchung von Containern* können Sie Container und Images auf Befehl untersuchen.

- **Schutz vor Web-Bedrohungen**. Mit der Komponente *Schutz vor Web-Bedrohungen* können Sie eingehenden Datenverkehr untersuchen, das Herunterladen schädlicher Dateien aus dem Internet verhindern und Phishing-, Adware- und andere gefährliche Websites blockieren. Kaspersky Endpoint Security kann geschützte Verbindungen untersuchen.

- **Schutz vor Netzwerkbedrohungen**. Mit der Komponente *Schutz vor Netzwerkbedrohungen* können Sie den eingehenden Netzwerkdatenverkehr auf Aktivitäten untersuchen, die für Netzwerkangriffe typisch sind.

- **Firewall-Verwaltung**. Mit der Komponente *Firewall-Verwaltung* können Sie die Firewall-Einstellungen des Betriebssystems überwachen und alle Netzwerkaktivitäten gemäß den von Ihnen konfigurierten Netzwerkpaketregeln filtern.

- **Schutz vor Verschlüsselung**. Mit der Komponente *Schutz vor Verschlüsselung* können Sie den Zugriff von Remote-Geräten auf Dateien in lokalen Verzeichnissen mit Netzwerkzugriff über SMB/NFS-Protokolle untersuchen und Dateien vor bösartiger Remote-Verschlüsselung schützen.

- **Gerätekontrolle**. Mit der Komponente *Gerätekontrolle* können Sie den Benutzerzugriff auf zusätzliche oder externe Geräte verwalten, die auf dem Client-Gerät installiert oder daran angeschlossen sind (z. B. Festplatten, Kameras oder WLAN-Module). Auf diese Weise können Sie das Client-Gerät vor einer Infektion schützen, wenn

Sie externe Geräte anschließen, und Datenverlust oder Datenlecks verhindern. Der Benutzerzugriff auf Geräte wird mithilfe des Zugriffsmodus und der von Ihnen konfigurierten Zugriffsregeln überwacht.

- **App-Kontrolle**. Mit der Komponente *App-Kontrolle* können Sie den Start von Apps auf Benutzergeräten überwachen. Dies reduziert das Infektionsrisiko von Geräten, da der Zugriff auf Apps eingeschränkt wird. Der Start von Apps wird mithilfe der von ihnen konfigurierten Regeln für die App-Kontrolle überwacht.

- **Inventarisierung**. Mithilfe der Aufgabe *Inventarisierung* erhalten Sie Informationen über alle ausführbaren Dateien der App, die auf den Client-Geräten gespeichert sind. Diese Informationen können nützlich sein, um z. B. Regeln für die App-Kontrolle zu erstellen.

- **Web-Kontrolle**. Die Komponente *Web-Kontrolle* steuert den Benutzerzugriff auf Webressourcen. Dies hilft bei der Reduzierung des verbrauchten Datenverkehrs und der Einschränkung von unangemessenen Tätigkeiten während der Arbeitszeit. Wenn ein Benutzer versucht, eine Website zu öffnen, deren Zugriff durch die Web-Kontrolle eingeschränkt ist, blockiert Kaspersky Endpoint Security den Zugriff oder zeigt eine Warnung an.

- **Verhaltensanalyse**. Mit der Komponente *Verhaltensanalyse* können Sie schädliche Aktivitäten von Apps im Betriebssystem überwachen. Wenn schädliche Aktivitäten erkannt werden, kann Kaspersky Endpoint Security den Prozess der App, welche die bösartigen Aktivitäten ausführt, beenden.

- Mit der **Überwachung der Systemintegrität** können Sie Änderungen an Dateien und Verzeichnissen des Betriebssystems überwachen. Die Komponente *Überwachung der Systemintegrität* überwacht in Echtzeit Aktionen, die mit Objekten in dem Überwachungsbereich durchgeführt werden, der in den Komponenteneinstellungen angegeben ist. Mithilfe der Aufgabe *Prüfung der Systemintegrität* können Sie die Systemintegrität auf Befehl untersuchen. Während der Prüfung wird der aktuelle Status der Objekte im Überwachungsbereich mit dem Originalstatus dieser Objekte verglichen, der zuvor als Baseline festgelegt wurde.

Mit Kaspersky Endpoint Security können Sie infizierte Objekte erkennen und in ihnen gefundene Bedrohungen beseitigen. Zu diesem Zweck kann die App Folgendes verwenden:

- App-Datenbanken zum Erkennen und Desinfizieren von infizierten Dateien. Während des Untersuchungsprozesses analysiert die App jede Datei auf Bedrohungen: Der Dateicode wird mit dem Code einer echten Bedrohung verglichen und auf mögliche Übereinstimmungen untersucht.

- Kaspersky Security Network. Mithilfe der Daten aus Kaspersky Security Network wird die Reaktion von Kaspersky Endpoint Security auf verschiedenste Bedrohungen beschleunigt, die Leistungsfähigkeit einiger Komponenten erhöht und das Risiko von Fehlalarmen reduziert.

Vor der Desinfektion oder dem Löschen speichert Kaspersky Endpoint Security Backup-Kopien von Dateien im Backup auf dem Gerät. Wenn aufgrund einer Desinfektion wichtige Informationen, die in einer Datei enthalten waren, vollständig oder teilweise verloren gegangen sind, können Sie die Datei aus ihrer Backup-Kopie wiederherstellen.

Während der Ausführung von Untersuchungsaufgaben kann Kaspersky Endpoint Security Dateien desinfizieren und löschen, die vor Änderungen geschützt sind: Dateien mit den Attributen "immutable" und "append-only" sowie Dateien in Verzeichnissen mit den Attributen "immutable" und "append-only". Im Backup werden Kopien dieser Dateien gespeichert, die vor der Desinfektion oder dem Löschen erstellt wurden. Bei Bedarf können Sie Dateien aus Backups wiederherstellen. Nach dem Abschluss der Untersuchungsaufgaben werden die Attribute "immutable" und "append-only" der desinfizierten Dateien zurückgesetzt.

Kaspersky Endpoint Security kann im informativen Modus ausgeführt werden. Der *informative Modus* ist ein Ausführungsmodus der App, in dem die Komponenten und Aufgaben der App bei Erkennung einer Bedrohung weder versuchen, schädliche Objekte zu desinfizieren, zu entfernen oder für Zugriffe sperren noch andere Programmaktivitäten zu blockieren. Stattdessen wird der Benutzer lediglich über die Erkennung einer Bedrohung informiert.

Kaspersky Endpoint Security unterstützt die Möglichkeit der Integration mit anderen Lösungen von Kaspersky, um die Funktionen der App zu erweitern:

- Die Integration mit Kaspersky Managed Detection and Response gewährleistet die kontinuierliche Suche, Erkennung und Beseitigung von Bedrohungen, die gegen Ihr Unternehmen gerichtet sind.
- Die Integration mit Kaspersky Endpoint Detection and Response (KATA), einer Komponente der Kaspersky Anti Targeted Attack Platform, gewährleistet den Schutz der IT-Infrastruktur des Unternehmens sowie die rechtzeitige Erkennung von Zero-Day-Bedrohungen, gezielten Angriffen und Advanced Persistent Threats.
- Die Integration mit Kaspersky Endpoint Detection and Response Optimum gewährleistet den Schutz der IT-Infrastruktur eines Unternehmens vor Bedrohungen wie Exploits, Ransomware, dateilosen Angriffen (fileless attacks) und dem bösartigen Ausnutzen legitimer System-Tools zur Beschädigung von Geräten und Daten.

Sie können Kaspersky Endpoint Security als Container-App (im Folgenden KESL-Container genannt) zur Integration in externe Systeme verwenden, um Container-Images in Repositories zu untersuchen.

Die Funktionalität für KESL-Container wird nicht unterstützt, wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden.

Um die App auf dem neuesten Stand zu halten, werden zusätzliche App-Funktionen bereitgestellt:

- Aktivierung der App mithilfe einer Schlüsseldatei oder eines Aktivierungscodes.

  Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, erfolgt die Aktivierung auf der Seite des Schutzservers (dies ist eine Komponente von Kaspersky Security for Virtualization Light Agent).

- Update der Datenbanken und Module der App über die Kaspersky-Update-Server, über den Administrationsserver oder über eine vom Benutzer angegebene Quelle nach Zeitplan oder auf Befehl.

  Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, erhält die App die Updates der Programmdatenbanken und Module vom Schutzserver (dies ist eine Komponente von Kaspersky Security for Virtualization Light Agent).

- Differenzierung des Benutzerzugriffs auf Funktionen der App entsprechend den Benutzerrollen.
- Benachrichtigung des Administrators über Ereignisse, die während der Ausführung der App aufgetreten sind.
- Integritätsprüfung der App-Komponenten mit dem Tool zur Integritätsprüfung.

Kaspersky Endpoint Security kann auf folgende Arten verwaltet werden:

- Mithilfe von Kaspersky Security Center über die Kaspersky Security Center Web Console, die Kaspersky Security Center Cloud Console oder die Verwaltungskonsole.
- Über die Befehlszeile mithilfe von Verwaltungsbefehlen.
- Über die grafische Benutzeroberfläche.

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, kann die App nicht über die Kaspersky Security Center Cloud Console und die grafische Benutzeroberfläche verwaltet werden.

Über die Nutzungsmodi von Kaspersky Endpoint Security

Sie können Kaspersky Endpoint Security in einem der folgenden Modi verwenden:

- Im Standard-Modus zum Schutz von Workstations und Server (im Weiteren auch "Standard-Modus"). Kaspersky Endpoint Security wird als autonome App zum Schutz von Geräten mit Linux-Betriebssystemen verwendet.
- Im Light Agent-Modus zum Schutz virtueller Umgebungen als ein Teil der Lösung Kaspersky Security for Virtualization Light Agent (im Weiteren auch "Light Agent-Modus"). Kaspersky Endpoint Security wird als Light Agent-Komponente von Kaspersky Security for Virtualization Light Agent für den Schutz von virtuellen Maschinen mit Linux-Gastbetriebssystemen verwendet.

Standardmäßig wird die App im Standard-Modus verwendet.

Wenn Sie die App im Light Agent-Modus verwenden möchten, müssen Sie die folgenden Schritte ausführen:

1. Installieren Sie Kaspersky Endpoint Security auf jeder virtuellen Maschine, die mit Kaspersky Security for Virtualization Light Agent geschützt werden soll. Sie können die App auch auf einer Vorlage für virtuelle Maschinen installieren.

   Während der Installation müssen Sie auf eine der folgenden Arten angeben, dass die App im Light Agent-Modus verwendet werden soll:

   - Während der Erstkonfiguration der App im interaktiven oder automatischen Modus (bei einer Installation über die Befehlszeile).
   - In den Eigenschaften des Installationspakets der App oder in der Konfigurationsdatei autoinstall.ini, die im Installationspaket enthalten ist (im Falle einer Installation mittels Kaspersky Security Center).

   Nach der Installation von Kaspersky Endpoint Security können Sie den Nutzungsmodus der App nicht mehr ändern.

   Wenn Sie den Light Agent-Modus auswählen, können Sie auch die folgenden Einstellungen für die Ausführung von Kaspersky Endpoint Security im Light Agent-Modus konfigurieren:

   - Die Rolle der virtuellen Maschine, die Sie in der virtuellen Infrastruktur schützen möchten: Server oder Workstation. Die Rolle der virtuellen Maschine legt fest, unter welcher Lizenz die App auf dieser virtuellen Maschine verwendet wird und wie groß der verfügbare Funktionsumfang ist.
   - Modus zum Schutz der VDI-Infrastruktur Es wird empfohlen, diesen Modus zu aktivieren, wenn Sie die App auf einer Vorlage für virtuelle Maschinen installieren, aus dem temporäre virtuelle Maschinen erstellt werden. Der Modus zum Schutz der VDI-Infrastruktur optimiert die Ausführung von Kaspersky Endpoint Security auf temporären virtuellen Maschinen.

2. Es können die Verbindungseinstellungen vom Light Agent zur SVM und vom Light Agent zum Integrationsserver konfiguriert werden.

Kaspersky Endpoint Security interagiert im Light Agent-Modus mit folgenden weiteren Komponenten von Kaspersky Security for Virtualization Light Agent: dem Integrationsserver und dem auf der SVM installierten Schutzserver (weitere Informationen dazu finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent). Um mit dem Schutzserver zu interagieren, stellt Kaspersky Endpoint Security zur der SVM mit dem installierten Schutzserver eine Verbindung her und erhält diese aufrecht.

Wenn Sie möchten, dass die Light Agents Informationen über die SVMs mittels des Integrationsservers erhalten, oder wenn Sie die Verbindung zwischen dem Schutzserver und dem Light Agent sichern möchten, ist eine Verbindung zum Integrationsserver erforderlich.

Sie können die Verbindungseinstellungen in den Einstellungen der Richtlinie von Kaspersky Endpoint Security entweder über die Verwaltungskonsole von Kaspersky Security Center oder über die Kaspersky Security Center Web Console konfigurieren.

Die Informationen über die Ausführungseinstellungen der App im Light Agent-Modus und über die Verbindungen zum Integrationsserver und zur SVM können Sie mit den folgenden App-Befehlen abrufen: `kesl-control --ksvla-info`, `kesl-control --viis-info` und `kesl-control --svm-info`.

Die Informationen über den Nutzungsmodus der App werden in Kaspersky Security Center in den App-Eigenschaften von Kaspersky Endpoint Security auf dem verwalteten Gerät im Abschnitt **Komponenten** angezeigt. Die folgenden Informationen werden in der Zeile **Light Agent-Modus zum Schutz virtueller Umgebungen** auf folgende Weise angezeigt:

- Der *Ausführungsstatus* gibt an, dass die App im Light Agent-Modus verwendet wird.
- Der Status *Nicht installiert* gibt an, dass die App im Standard-Modus verwendet wird.

Informationen zum Aktivieren der App im Light Agent-Modus

Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, müssen Sie die App nicht separat aktivieren. Sie aktivieren Kaspersky Security for Virtualization Light Agent. Die Aktivierung erfolgt auf der Seite des Schutzservers (dies ist eine Komponente von Kaspersky Security for Virtualization Light Agent) durch das Hinzufügen eines Lizenzschlüssels auf der SVM. Weitere Informationen finden Sie in der Hilfe von Kaspersky Security for Virtualization Light Agent.

Um die Funktionalität von Kaspersky Endpoint Detection and Response Optimum zu aktivieren, muss der SVM zusätzlich einen Lizenzschlüssel für EDR Optimum hinzugefügt werden. Die Lizenzen zur Aktivierung der Komponenten von Kaspersky Security for Virtualization Light Agent decken diese Funktionalität nicht ab.

Nach der Aktivierung der Lösung und der Verbindung des Light Agent mit der SVM übermittelt der Schutzserver die Lizenzinformationen an den Light Agent. Bei der Auswahl einer SVM für die Verbindung berücksichtigt der Light Agent neben weiteren Parametern auch den Typ des Lizenzschlüssels, welcher der SVM hinzugefügt wurde. Der Light Agent stellt keine Verbindung zur SVM her, wenn der Schlüssel, welcher der SVM hinzugefügt wurde, nicht der Rolle der geschützten virtuellen Maschine in der virtuellen Infrastruktur (Server oder Workstation) entspricht. Weitere Informationen finden Sie in der Hilfe von Kaspersky Security for Virtualization Light Agent.

Die Informationen über die von Light Agent for Linux verwendete Lizenz können Sie auf einer geschützten virtuellen Maschine mit installiertem Light Agent mit dem folgenden Befehl abrufen: `kest-control -L --query`.

Die folgenden Methoden zur Verwaltung von Lizenzschlüsseln werden nicht unterstützt: Mithilfe der Aufgabe *Hinzufügen eines Schlüssels* von Kaspersky Endpoint Security und mithilfe der Befehle von Kaspersky Endpoint Security zum Hinzufügen und Entfernen von Lizenzschlüsseln.

Informationen zum Aktualisieren von Datenbanken und App-Modulen im Light Agent-Modus

Kaspersky Endpoint Security verwendet im Light Agent-Modus spezielle Malware-Datenbanken, die für die Ausführung der App im Rahmen von Kaspersky Security for Virtualization Light Agent erforderlich sind. Kaspersky Endpoint Security erhält vom Schutzserver Updates für die Datenbanken und Programm-Module. Weitere Informationen finden Sie in der Hilfe von Kaspersky Security for Virtualization Light Agent.

Die Datenbanken und Module auf geschützten virtuellen Maschinen werden mithilfe einer speziellen lokalen *Update*-Aufgabe in Kaspersky Endpoint Security aktualisiert, bei welcher der Ordner auf der SVM als Update-Quelle angegeben wird. Diese Update-Aufgabe wird automatisch gestartet. Sie können diese Aufgabe weder löschen noch ihre Einstellungen ändern.

Die Aktualisierung aus Quellen, die nicht dem Ordner auf der SVM entsprechen, und die Verwendung von Update-Gruppenaufgaben werden nicht unterstützt.

Das Rollback des letzten Updates für Malware-Datenbanken wird ebenfalls auf der Seite des Schutzservers durchgeführt. Nach dem Rollback des Datenbanken-Updates und der App-Module auf der SVM, startet auf der geschützten virtuellen Maschine automatisch eine spezielle lokale *Update*-Aufgabe. Nach Abschluss dieser Aufgabe kehrt der Light Agent zur Verwendung des vorherigen Satzes von Malware-Datenbanken zurück.

Die Verwendung von lokalen Aufgaben und Gruppenaufgaben des Typs *Rollback des Datenbanken-Updates* von Kaspersky Endpoint Security wird nicht unterstützt.

Weitere Besonderheiten bei der Verwendung der App im Light Agent-Modus

Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird:

- Wird die Funktion für KESL-Container nicht unterstützt.
- Die App kann weder über die Kaspersky Security Center Cloud Console noch über die grafische Benutzeroberfläche verwaltet werden.
- Wird die Verwendung von cloud-basierten Datenbanken nicht unterstützt.
- Kaspersky Endpoint Security interagiert über den KSN-Proxy-Server mit den KSN-Servern. Die direkte Interaktion mit KSN wird nicht unterstützt.
- Wird die Verwendung des Proxy-Servers der App bei einer Verbindung zum Integrationsserver, zur SVM oder zu KSN-Servern nicht unterstützt.
- Die Integration mit Kaspersky Symphony XDR wird nicht unterstützt.

Lieferumfang

Auf der Website von Kaspersky können Sie die Dateien herunterladen, die zum Lieferumfang von Kaspersky Endpoint Security gehören, sowie die Dateien, die von Kaspersky Security Center für die Remote-Installation dieser App verwendet werden.

Der Lieferumfang umfasst das Installationspaket der App Kaspersky Endpoint Security mit den folgenden Dateien:

- kesl-12.1.0-<Build-Nummer>.i386.rpm, kesl_12.1.0-<Build-Nummer>_i386.deb

Enthalten die Hauptdateien der App. Die Pakete können auf 32-Bit-Betriebssystemen auf der Grundlage des Typs des Paketmanagers installiert werden.

- kesl-12.1.0-<Build-Nummer>.x86_64.rpm, kesl_12.1.0-<Build-Nummer>_amd64.deb

  Enthalten die Hauptdateien der App. Die Pakete können auf 64-Bit-Betriebssystemen auf der Grundlage des Typs des Paketmanagers installiert werden.

- kesl-12.1.0-<Build-Nummer>.aarch64.rpm, kesl_12.1.0-<Build-Nummer>_arm64.deb

  Enthalten die Hauptdateien der App. Die Pakete können auf 64-Bit-Betriebssystemen für Arm®-Architektur auf der Grundlage des Typs des Paketmanagers installiert werden.

- kesl-gui-12.1.0-<Build-Nummer>.i386.rpm, kesl-gui_12.1.0-<Build-Nummer>_i386.deb

  Enthalten die Dateien der grafischen Benutzeroberfläche der App. Die Pakete können auf 32-Bit-Betriebssystemen auf der Grundlage des Typs des Paketmanagers installiert werden.

- kesl-gui-12.1.0-<Build-Nummer>.x86_64.rpm, kesl-gui_12.1.0-<Build-Nummer>_amd64.deb

  Enthalten die Dateien der grafischen Benutzeroberfläche der App. Die Pakete können auf 64-Bit-Betriebssystemen auf der Grundlage des Typs des Paketmanagers installiert werden.

- kesl-gui-12.1.0-<Build-Nummer>.aarch64.rpm, kesl-gui_12.1.0-<Build-Nummer>_arm64.deb

  Enthalten die Dateien der grafischen Benutzeroberfläche der App. Die Pakete können auf 64-Bit-Betriebssystemen für Arm-Architektur auf der Grundlage des Typs des Paketmanagers installiert werden.

- kesl-12.1.0.<Build-Nummer>.zip

  Enthält die Dateien, die während der Remote-Installation der App über Kaspersky Security Center verwendet werden, darunter die Dateien license.<Sprach-ID> und ksn_license.<Sprach-ID>.

  > Der Kaspersky Security Center Administrationsagent ist nicht im Lieferumfang enthalten. Sie können ihn von Download-Seite der App im Abschnitt **Kaspersky Security Center** herunterladen.

- docker-service-kesl64-12.1.0-<Build-Nummer>.tgz

  Enthält Dateien zum Erstellen des Images der Container-App KESL-Container.

- ksn_license.<ID der Sprache>

  Enthält den Text der Erklärung zu Kaspersky Security Network.

- license.<ID der Sprache>

  Enthält den Text des Endbenutzer-Lizenzvertrags. Der Endbenutzer-Lizenzvertrag enthält die Bedingungen für die Nutzung der App.

Wenn die App-Dateien auf eine andere Weise geändert werden, als in der Dokumentation zur App oder in den Anleitungen der Support-Experten beschrieben, kann die App oder das Betriebssystem verlangsamt oder negativ beeinträchtigt werden. Das Schutzniveau Ihres Gerätes kann sich verringern und der Zugriff auf die Integrität von verarbeiteten Informationen, einschließlich der zusätzlich übertragenen KSN-Statistiken, kann beschädigt werden.

Hardware- und Softwarevoraussetzungen

Dieser Abschnitt enthält die Hardware- und Softwarevoraussetzungen von Kaspersky Endpoint Security.

Hardwarevoraussetzungen

Für die App Kaspersky Endpoint Security müssen folgende Hardwarevoraussetzungen erfüllt sein:

Die Mindest-Hardwarevoraussetzungen:

- Prozessor Core™ 2 Duo 1,86 GHz oder höher
- Mindestens 1 GB für die Swap-Partition
- 1 GB RAM für 32-Bit-Betriebssysteme und 2 GB RAM für 64-Bit-Betriebssysteme
- 4 GB freier Speicher auf der Festplatte für die Installation der App und zur Speicherung von temporären Dateien und Protokolldateien
- Bei Verwendung der grafischen Benutzeroberfläche, muss der Monitor die Fenster in einer Breite von 1000 Pixeln und einer Höhe von 600 Pixeln darstellen können (Wenn eine Bildschirmskalierung angewendet wird, werden diese Abmessungen ebenfalls skaliert).
- Bei Verwendung von Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen wird eine virtuelle Netzwerkschnittstelle mit einer Bandbreite von 100 Mbit/s benötigt

Minimale Hardwareanforderungen für die Arm-Architektur:

- Prozessor Armv8.2-A Kunpeng 920 oder Armv8-A Baikal-M (BE-M1000) oder m-Trust Terminal
- Mindestens 1 GB für die Swap-Partition
- 2 GB RAM
- 3 GB freier Speicher auf der Festplatte für die Installation der App und zur Speicherung von temporären Dateien und Protokolldateien
- Bei Verwendung der grafischen Benutzeroberfläche, muss der Monitor die Fenster in einer Breite von 1000 Pixeln und einer Höhe von 600 Pixeln darstellen können (Wenn eine Bildschirmskalierung angewendet wird, werden diese Abmessungen ebenfalls skaliert).

Die Verwendung von Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen wird auf Betriebssystemen mit Arm-Architektur nicht unterstützt.

Softwarevoraussetzungen

Um Kaspersky Endpoint Security auf zu installieren, muss auf dem Gerät eins der folgenden Betriebssysteme installiert sein:

- 32-Bit-Betriebssysteme:
  - Debian GNU/Linux 11.0 und höher
  - Debian GNU/Linux 12.0 und höher
  - Mageia™ 4

    Auf Geräten mit dem Betriebssystem Mageia 4 wird die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response (KATA) nicht unterstützt.

  - ALT 8 SP Workstation (8.4)
  - ALT 8 SP Server (8.4)
  - ALT SP Workstation Release 10
  - ALT SP Server Version 10
- 64-Bit-Betriebssysteme:
  - Alma Linux OS 8 und höher
  - Alma Linux OS 9 und höher
  - AlterOS® 7.5 und höher
  - Amazon™ Linux 2
  - Astra Linux Common Edition Orel 2.12
  - Astra Linux Special Edition RUSB.10015-01 (operational Update 1.5)
  - Astra Linux Special Edition RUSB.10015-01 (operational Update 1.6)
  - Astra Linux Special Edition RUSB.10015-01 (operational Update 1.7)
  - Astra Linux Special Edition RUSB.10015-16 (Release 1) (operational Update 1.6)

    Auf Geräten mit den Betriebssystemen Astra Linux in den Modi für Mandatory Access Control und für geschlossene Softwareumgebung wird die Verwendung von Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen nicht unterstützt.

  Auf einem Tablet-Computer (Tablet) im Modus "Mobile" ausgeführtes Astra-Betriebssystem wird nur Desktop-Modus unterstützt.

  - CentOS 7.2 und höher
  - CentOS Stream 8
  - CentOS Stream 9

- Debian GNU/Linux 11.0 und höher
- Debian GNU/Linux 12.0 und höher
- EMIAS 1.0 und höher
- EulerOS 2.0 SP10
- Kylin 10
- Linux Mint 20.3 und höher
- Linux Mint 21.1 und höher
- openSUSE Leap 15.0 und höher
- Oracle Linux 7.3 und höher
- Oracle Linux 8.0 und höher
- Oracle Linux 9.0 und höher
- Red Hat Enterprise Linux 7.2 und höher
- Red Hat Enterprise Linux 8.0 und höher
- Red Hat Enterprise Linux 9.0 und höher
- Rocky Linux 8.5 und höher
- Rocky Linux 9.1
- SberLinux 8.8 (Dykhtau)
- SberOS 3.2.0.
- SUSE Linux Enterprise Server 12.5 und höher
- SUSE Linux Enterprise Server 15 und höher
- Ubuntu® 20.04 LTS
- Ubuntu 22.04 LTS
- Ubuntu 24.04 LTS
- ALT 8 SP Workstation (8.4)
- ALT 8 SP Server (8.4)
- ALT Education 10.1
- ALT Workstation 10.1
- ALT Server 10.1

- ALT SP Workstation Release 10
- ALT SP Server Version 10
- Atlant, Build Alcyone, Version 2022.02
- GosLinux 7.17
- GosLinux 7.2
- MSVSPHERE 9.2 ARM
- MSVSPHERE 9.2 SERVER
- RED OS® 7.3
- RED OS 8.0
- ROSA "Kobalt" 7.9
- ROSA "Chrom" 12
- SintezM-Client 8.6
- SintezM-Server 8.6

- 64-Bit-Betriebssysteme für die ARM-Architektur:
  - Astra Linux Special Edition RUSB.10152-02 (reguläres Update 4.7)
  - CentOS Stream 9
  - EulerOS 2.0 SP10
  - SUSE Linux Enterprise Server 15
  - Ubuntu 22.04 LTS
  - ALT 8 SP Workstation (8.4)
  - ALT 8 SP Server (8.4)
  - ALT SP Workstation Release 10
  - ALT SP Server Version 10
  - RED OS 7.3

Auf Geräten mit den Betriebssystemen für Arm-Architektur wird die Verwendung von Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen nicht unterstützt.

Aufgrund von Einschränkungen der fanotify-Technologie, werden die folgenden Dateisysteme von der App nicht unterstützt: autofs, binfmt_misc, cgroup, configfs, debugfs, devpts, devtmpfs, fuse, fuse.gvfsd-fuse, gfs2, gvfs, hugetlbfs, mqueue, nfsd, proc, parsecfs, pipefs, pstore, usbfs, rpc_pipefs, securityfs, selinuxfs, sysfs, tracefs.

Unterstützte Versionen von Kaspersky Security Center

Kaspersky Endpoint Security unterstützt die folgenden Versionen von Kaspersky Security Center:

- Kaspersky Security Center 13.2. Die Verwaltung der App Kaspersky Endpoint Security über die Verwaltungskonsole mithilfe des mmc-Verwaltungs-Plugins wird unterstützt.
- Kaspersky Security Center 14. Die Verwaltung von Kaspersky Endpoint Security über die Verwaltungskonsole mithilfe des MMC-basierten Verwaltungs-Plug-ins und über die Kaspersky Security Center Web Console mithilfe des Web-Verwaltungs-Plug-ins wird unterstützt.
- Kaspersky Security Center 14.2 Windows. Die Verwaltung von Kaspersky Endpoint Security über die Verwaltungskonsole mithilfe des MMC-basierten Verwaltungs-Plug-ins und über die Kaspersky Security Center Web Console mithilfe des Web-Verwaltungs-Plug-ins wird unterstützt.
- Kaspersky Security Center 14.2 Linux. Die Verwaltung von Kaspersky Endpoint Security über die Kaspersky Security Center Web Console mithilfe des Web-Verwaltungs-Plug-ins wird unterstützt.
- Kaspersky Security Center 15 Linux. Die Verwaltung von Kaspersky Endpoint Security über die Kaspersky Security Center Web Console mithilfe des Web-Verwaltungs-Plug-ins wird unterstützt.
- Kaspersky Security Center 15.1 Linux. Die Verwaltung von Kaspersky Endpoint Security über die Kaspersky Security Center Web Console mithilfe des Web-Verwaltungs-Plug-ins wird unterstützt.

Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird (als Teil von Kaspersky Security for Virtualization Light Agent), wird es empfohlen, die folgenden Versionen von Kaspersky Security Center zur Verwaltung der App zu verwenden:

- Kaspersky Security Center 14.2 Windows.
- Kaspersky Security Center 15 Linux.
- Kaspersky Security Center 15.1 Linux.

Die Verwaltung von Kaspersky Endpoint Security über Kaspersky Security Center erfordert den Administrationsagenten von Kaspersky Security Center.

Der Kaspersky Security Center Administrationsagent ist nicht im Lieferumfang von Kaspersky Endpoint Security enthalten. Sie können ihn von Download-Seite der App im Abschnitt **Kaspersky Security Center** herunterladen.

Wenn Sie die Anwendungsintegration mit Kaspersky Endpoint Detection and Response (KATA) verwenden, wird es empfohlen, die folgenden Versionen von Kaspersky Security Center zur Verwaltung der App zu verwenden:

- Kaspersky Security Center 14.2 Windows.

- Kaspersky Security Center 15 Linux.
- Kaspersky Security Center 15.1 Linux.

Unterstützte Versionen von Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Security unterstützt die folgenden Versionen der Kaspersky Anti Targeted Attack Platform:

- Kaspersky Anti Targeted Attack Platform 5.1 Wird eingeschränkt unterstützt.
- Kaspersky Anti Targeted Attack Platform 6.0
- Kaspersky Anti Targeted Attack Platform 6.1

Weitere Informationen über Kaspersky Anti Targeted Attack Platform finden Sie in der Hilfe zu Kaspersky Anti Targeted Attack Platform.

Neuerungen

Kaspersky Endpoint Security bietet jetzt die folgenden Möglichkeiten und Verbesserungen:

- Es ist nun möglich, die Anwendung mit Kaspersky Endpoint Detection and Response Optimum zu integrieren, um den Schutz der IT-Infrastruktur eines Unternehmens vor Bedrohungen wie Exploits, Ransomware, dateilosen Angriffen (fileless attacks) und dem bösartigen Ausnutzen legitimer System-Tools zur Beschädigung von Geräten und Daten zu gewährleisten.

- Es ist nun möglich, der App zwei aktive Lizenzschlüssel hinzuzufügen: einen Hauptschlüssel zum Aktivieren der App und einen zusätzlichen Schlüssel zum Aktivieren der Funktionalität von Kaspersky Endpoint Detection and Response Optimum. Ein zusätzlicher Schlüssel ist erforderlich, wenn Ihre Hauptlizenz die Funktionalität von Kaspersky Endpoint Detection and Response Optimum nicht umfasst.

- Es wurde die neue Funktionskomponente *Web-Kontrolle* hinzugefügt, die den Benutzerzugriff auf Webressourcen steuert. Dies hilft bei der Reduzierung des verbrauchten Datenverkehrs und der Einschränkung von unangemessenen Tätigkeiten während der Arbeitszeit. Wenn ein Benutzer versucht, eine Website zu öffnen, deren Zugriff durch die Web-Kontrolle eingeschränkt ist, blockiert Kaspersky Endpoint Security den Zugriff oder zeigt eine Warnung an.

- Es wurde eine Funktion zur Überwachung der Stabilität von Kaspersky Endpoint Security implementiert, mit der Sie die Anzahl der ungeplanten Unterbrechungen der App verfolgen und den Administrator über den instabilen Betrieb der App informieren können.

- Das Verfahren zur Installation von Kaspersky Endpoint Security mithilfe der Kaspersky Security Center Web Console wurde verbessert: In den Eigenschaften des Installationspakets der App können Sie jetzt die Einstellungen für die Erstkonfiguration der App angeben, die bisher nur in der Konfigurationsdatei "autoinstall.ini" verfügbar waren.

- Die Möglichkeit, zusätzliche App-Einstellungen über die Kaspersky Security Center Web Console und die Kaspersky Security Center Verwaltungskonsole zu verwalten, wurde erweitert: Sie können Einstellungen konfigurieren, die bisher nur über die Konfigurationsdatei "kesl.ini" konfiguriert werden konnten.

- Es wurde eine Option hinzugefügt, die Verwendung von globalen Ausschlüssen und von Ausschlüssen aus dem Schutz vor bedrohlichen Dateien während der Ausführung von Untersuchungsaufgaben zu aktivieren und zu deaktivieren.

- Es wurde die Möglichkeit der Integration mit Kaspersky Symphony XDR implementiert: Wenn Kaspersky Endpoint Security im Standard-Modus verwendet wird, kann die App Reaktionsmaßnahmen vom Typ "Start der Schadsoftware-Untersuchung" und "Datenbanken-Update" ausführen. Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, wird die Integration mit Kaspersky Symphony XDR nicht unterstützt.

- Wenn die App mit Kaspersky Security Center verwaltet wird, werden Informationen über alle auf den Client-Geräten installierten oder mit ihnen verbundenen Geräte (einschließlich der zuvor installierten und verbundenen sowie der bereits getrennten Geräte) künftig an den Administrationsserver übertragen.

- Die Regeln zum Abfangen des Datenverkehrs wurden verbessert, um die Interaktion von Containern im selben Netzwerk zu unterstützen.

- Die Liste der unterstützten Betriebssysteme wurde aktualisiert.

Vorbereitung der Installation von Kaspersky Endpoint Security

Allgemeine Maßnahmen

Bevor Sie mit der Installation von Kaspersky Endpoint Security beginnen, gehen Sie wie folgt vor:

- Überprüfen Sie, ob Ihr Gerät die Hardware- und Softwareanforderungen der App erfüllt.
- Stellen Sie sicher, dass auf Ihrem Gerät keine Antivirensoftware von Drittanbietern installiert ist.
- Stellen Sie sicher, dass Kaspersky Endpoint Agent für Linux nicht auf Ihrem Gerät installiert ist. Wenn Kaspersky Endpoint Agent für Linux installiert ist, erscheint während der Installation eine Meldung, in der Sie aufgefordert werden, es manuell zu deinstallieren.
- Stellen Sie sicher, dass auf Ihrem Gerät der Perl-Interpreter ab Version 5.10 installiert ist.
- Stellen Sie auf Geräten mit Betriebssystemen ohne Unterstützung der Fanotify-Technologie sicher, dass Folgendes installiert ist:
  - Pakete zur Programmkompilierung und Aufgabenausführung (gcc, binutils, glibc, glibc-devel, make, ld, rpcbind).
  - Paket mit Kernel-Header-Dateien des Betriebssystems zum Kompilieren der Module von Kaspersky Endpoint Security.
- Installieren Sie je nach Betriebssystem auf Ihrem Gerät eines der folgenden Pakete:
  - Auf einem Gerät mir dem Betriebssystem SUSE Linux Enterprise Server 15 das Paket "insserv-compat".
  - Auf einem Gerät mit dem Betriebssystem Red Hat Enterprise Linux 8 oder RED OS das Paket "perl-Getopt-Long".
  - Auf einem Gerät mit dem Betriebssystem Red Hat Enterprise Linux oder RED OS das Paket "perl-File-Copy". Dieses Paket ist für das Skript zur Ersteinrichtung der App notwendig, ist aber möglicherweise nicht im Betriebssystem enthalten.
- In Astra Linux Betriebssystemen ist das Verbot von ptrace-Protokollierung (Disable ptrace capability) standardmäßig aktiviert, das sich auf die Ausführung der App Kaspersky Endpoint Security auswirken kann. Für den korrekten Betrieb von Kaspersky Endpoint Security wird empfohlen, das ptrace-Protokollierungsverbot bei der Installation von Astra Linux zu deaktivieren. Wenn Astra Linux bereits installiert ist, finden Sie Anweisungen zum Aktivieren und Deaktivieren dieses Modus auf der Astra Linux Help Center-Website (**Schutz- und Blockier-Mechanismen konfigurieren**, Abschnitt **Ptrace-Protokollierung blockieren**).
- Wenn auf Ihrem Gerät ein Linux-Kernel unter Version 3.16 verwendet wird, müssen Sie sicherstellen, dass der Dienst auditd nicht gestartet oder installiert ist, damit die Integration mit Kaspersky Endpoint Detection and Response (KATA) ausgeführt wird.
- Damit die Komponenten Firewall-Verwaltung, Schutz vor Web-Bedrohungen und Schutz vor Netzwerkbedrohungen funktionieren, müssen Sie das Tool "iptables" auf Ihrem Gerät installieren.
- Zur Ausführung des Verwaltungs-Plug-ins für Kaspersky Endpoint Security muss auf dem Gerät mit dem Administrationsserver das Paket Microsoft® Visual C ++ 2015 Redistributable Update 3 RC installiert sein (siehe auch https://www.microsoft.com/de-de/download/details.aspx?id=52685)

- Um die App zu starten und auszuführen, muss sichergestellt werden, dass das root-Benutzerkonto der Besitzer für die folgenden Verzeichnisse ist, und dass ausschließlich der Besitzer Schreibrechte für sie besitzt: /var, /var/opt, /var/opt/kaspersky, /var/log/kaspersky, /opt, /opt/kaspersky, /usr/bin, /usr/lib, /usr/lib64.

Zusätzliche Maßnahmen vor der Installation von Kaspersky Endpoint Security im Light Agent-Modus

Wenn Sie vorhaben, Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen zu verwenden (im Rahmen von Kaspersky Security for Virtualization Light Agent), müssen Sie vor der Installation von Kaspersky Endpoint Security zusätzlich die folgenden Maßnahmen durchführen:

- Stellen Sie sicher, dass auf den zu schützenden virtuellen Maschinen die folgenden Pakete in abhängig von der virtuellen Infrastruktur, in der Kaspersky Security for Virtualization Light Agent bereitgestellt wird, installiert sind:
  - In einer Microsoft Hyper-V-Infrastruktur muss auf virtuellen Maschinen das Paket des Integrationsdienstes (Integration Services) installiert sein.
  - In einer VMware vSphere-Infrastruktur müssen auf virtuellen Maschinen die VMware Tools installiert sein.
  - In einer XenServer-Infrastruktur müssen auf virtuellen Maschinen die XenTools installiert sein.
  - In einer HUAWEI FusionSphere-Infrastruktur müssen auf virtuellen Maschinen die HUAWEI Tools installiert sein.
  - In einer Infrastruktur von KVM, OpenStack, VK Cloud Platform, TIONICS Cloud Platform, OpenStack, Astra Linux und ALT Virtualization Server muss auf virtuellen Maschinen der QEMU Guest Agent installiert sein.
- Stellen Sie sicher, dass in den Einstellungen Ihrer Netzwerkausrüstung oder der Software, die den Datenverkehr zwischen den virtuellen Maschinen steuert, die Durchleitung des Netzwerkdatenverkehrs über jene Ports zugelassen ist, die für die Interaktion von Kaspersky Endpoint Security im Light Agent-Modus mit den weiteren Komponenten von Kaspersky Security for Virtualization Light Agent verwendet werden. Weitere Informationen zu den Komponenten der Lösung finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

Ports für die Verwendung im Light Agent-Modus

Port und Protokoll	Richtung	Zweck und Beschreibung
7271 TCP	Vom Light Agent zum Integrationsserver.	Für die Interaktion zwischen Light Agent und dem Integrationsserver.
8000 UDP	Von der SVM zum Light Agent.	Für das Übertragen von Informationen über verfügbare SVMs an Light Agents mithilfe einer Liste von SVM-Adressen.
8000 UDP	Vom Light Agent zur SVM.	Für das Abrufen der Statusinformationen der SVM durch den Light Agent.
11111 TCP	Vom Light Agent zur SVM.	Für das Übertragen von Dienstanfragen (z. B. Abrufen von Lizenzinformationen) vom Light Agent an den Schutzserver während einer ungesicherten Verbindung.
11112 TCP	Vom Light Agent zur SVM.	Für das Übertragen von Dienstanfragen (z. B. Abrufen von Lizenzinformationen) vom Light Agent an den Schutzserver während einer gesicherten Verbindung.
9876 TCP	Vom Light Agent zur SVM.	Für das Übertragen von Anfragen zur Untersuchung von Dateien vom Light Agent an den Schutzserver während einer ungesicherten Verbindung.

9877 TCP	Vom Light Agent zur SVM.	Für das Übertragen von Anfragen zur Untersuchung von Dateien vom Light Agent an den Schutzserver während einer gesicherten Verbindung.
80 TCP	Vom Light Agent zur SVM.	Für das Aktualisieren der Datenbanken und App-Module der Lösung auf dem Light Agent.
15000 UDP	Von Kaspersky Security Center zur SVM.	Für die Verwaltung des Schutzservers durch Kaspersky Security Center.
15000 UDP	Von Kaspersky Security Center zu den Light Agents.	Für die Verwaltung der Light Agents durch Kaspersky Security Center.
13000 TCP	Vom Light Agent zu Kaspersky Security Center.	Zur Verwaltung von Light Agent durch Kaspersky Security Center während einer gesicherten Verbindung.
14000 TCP	Vom Light Agent zu Kaspersky Security Center.	Zur Verwaltung von Light Agent durch Kaspersky Security Center während einer ungesicherten Verbindung.

Installation und Erstkonfiguration von Kaspersky Endpoint Security

Bevor Sie mit der Installation von Kaspersky Endpoint Security beginnen, müssen Sie die Installation vorbereiten.

Die folgenden Szenarien beschreiben die Installation und Erstkonfiguration von Kaspersky Endpoint Security, sowie die Installation und Konfiguration des Administrationsagenten von Kaspersky Security Center und die Installation der Verwaltungs-Plug-ins von Kaspersky Endpoint Security. Das Installationsszenario hängt von dem Modus ab, in dem Sie Kaspersky Endpoint Security verwenden möchten.

Standard-Modus

Wenn Sie Kaspersky Endpoint Security im Standard-Modus verwenden möchten, umfasst die Installationsprozedur und Erstkonfiguration der App die folgenden Schritte:

1. **Installation und Erstkonfiguration des Administrationsagenten**

   Wenn Sie vorhaben, Kaspersky Endpoint Security mittels Kaspersky Security Center zur verwalten, installieren Sie auf dem geschützten Gerät den Kaspersky Security Center Administrationsagenten und konfigurieren Sie dessen Einstellungen.

2. **Verwaltungs-Plug-in für Kaspersky Endpoint Security installieren**

   Wenn Sie vorhaben, Kaspersky Endpoint Security mittels Kaspersky Security Center verwalten möchten, installieren Sie das Verwaltungs-Plugin für Kaspersky Endpoint Security. Je nach Verwaltungskonsole von Kaspersky Security Center werden die folgenden Verwaltungs-Plug-Ins verwendet:

   - Mit dem Web-Verwaltungs-Plug-in für Kaspersky Endpoint Security lässt sich die App über die Kaspersky Security Center Cloud Console und die Kaspersky Security Center Web Console verwalten. Das Web-Plug-in muss auf dem Gerät installiert werden, auf dem die Kaspersky Security Center Web Console installiert ist.

   - Mit dem MMC-Plug-in für die Verwaltung von Kaspersky Endpoint Security können Sie die App über die Verwaltungskonsole von Kaspersky Security Center verwalten. Das mmc-Plugin muss auf dem Gerät installiert werden, auf dem die Kaspersky Security Center Verwaltungskonsole installiert ist.

3. **App-Pakete und grafische Benutzeroberfläche installieren**

   Kaspersky Endpoint Security wird in den Paket-Formaten DEB und RPM bereitgestellt. Es sind spezielle Pakete für die App und die grafische Benutzeroberfläche vorgesehen. Installieren Sie Kaspersky Endpoint Security und, sofern notwendig, die grafische Benutzeroberfläche aus den Paketen des gewünschten Formats.

   Sie können die Installation auf eine der folgenden Arten durchführen:

   - Über Kaspersky Security Center.

   - Über die Befehlszeile.

4. **Erstkonfiguration von Kaspersky Endpoint Security**

   Die Erstkonfiguration muss ausgeführt werden, um den Schutz der Client-Geräte zu aktivieren.

   Wenn Sie die Kaspersky Endpoint Security mithilfe von Kaspersky Security Center installiert haben, bereiten Sie die App nach der Installation für die Ausführung vor.

   Wenn Sie Kaspersky Endpoint Security über die Befehlszeile installiert haben, starten Sie nach der Installation das Skript zur Erstkonfiguration oder führen Sie die Erstkonfiguration im automatischen Modus aus.

Light Agent-Modus

Die Verwendung von Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen wird auf Betriebssystemen mit Arm-Architektur nicht unterstützt.

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Maschinen verwenden möchten, umfasst die Installationsprozedur und Erstkonfiguration der App die folgenden Schritte:

1. **Installation und Erstkonfiguration des Administrationsagenten**

   Installieren Sie auf den virtuellen Maschinen und den Vorlagen für virtuelle Maschinen den Administrationsagenten von Kaspersky Security Center und konfigurieren Sie dessen Einstellungen.

   Wenn Sie den Administrationsagenten auf einer Vorlage installieren, aus der temporäre virtuelle Maschinen erstellt werden, wird es empfohlen, die Einstellungen so zu konfigurieren, dass die Leistung der temporären virtuellen Maschinen optimiert wird. Weitere Informationen über Installation virtueller Maschinen auf einer Vorlage finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

2. **Verwaltungs-Plug-in für Kaspersky Endpoint Security installieren**

   Installieren Sie das Verwaltungs-Plug-in für Kaspersky Endpoint Security. Je nach Verwaltungskonsole von Kaspersky Security Center werden die folgenden Verwaltungs-Plug-Ins verwendet:

   - Mit dem Web-Verwaltungs-Plug-in für Kaspersky Endpoint Security lässt sich die App über die Kaspersky Security Center Cloud Console und die Kaspersky Security Center Web Console verwalten. Das Web-Plug-in muss auf dem Gerät installiert werden, auf dem die Kaspersky Security Center Web Console installiert ist.
   - Mit dem MMC-Plug-in für die Verwaltung von Kaspersky Endpoint Security können Sie die App über die Verwaltungskonsole von Kaspersky Security Center verwalten. Das mmc-Plugin muss auf dem Gerät installiert werden, auf dem die Kaspersky Security Center Verwaltungskonsole installiert ist.

3. **Installation von App-Paketen und Erstkonfiguration von Kaspersky Endpoint Security**

   Kaspersky Endpoint Security wird in den Paket-Formaten DEB und RPM bereitgestellt. Installieren Sie Kaspersky Endpoint Security aus einem Paket im gewünschten Format. Es sind spezielle Pakete für die App und die grafische Benutzeroberfläche vorgesehen.

   Die grafische Benutzeroberfläche wird nicht unterstützt, wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden.

   Sie können die App auf eine der folgenden Arten installieren:

   - Über Kaspersky Security Center.

     Bevor Sie mit der Installation beginnen, müssen Sie die Einstellungen für die Ersteinrichtung der App auf eine der folgenden Arten konfigurieren:

     - In den Eigenschaften des Installationspakets auf der Registerkarte **Einstellungen** (diese Methode ist nur in der Kaspersky Security Center Web Console verfügbar).
     - Mithilfe der Konfigurationsdatei, die im Installationspaket enthalten ist.

     Sie müssen den Light Agent-Modus auswählen (entspricht dem Parameter `KSVLA_MODE=yes` in der Konfigurationsdatei). Wenn Sie Kaspersky Endpoint Security auf einer Vorlage installieren, aus der temporäre virtuelle Maschinen erstellt werden, wird es empfohlen, auch den Modus zum Schutz der VDI-Infrastruktur zu aktivieren. Dies optimiert die App-Ausführung auf temporären virtuellen Maschinen (entspricht dem Parameter `VDI_MODE=yes` in der Konfigurationsdatei).

   - Über die Befehlszeile. Wenn Sie die Installation über die Befehlszeile durchführen, wählen Sie bei der Erstkonfiguration aus, in welchem Modus Sie die App verwenden möchten.

4. **Erstkonfiguration von Kaspersky Endpoint Security**

   Die Erstkonfiguration muss ausgeführt werden, um den Schutz der Client-Geräte zu aktivieren.

   Wenn Sie die Kaspersky Endpoint Security mithilfe von Kaspersky Security Center installiert haben, bereiten Sie die App nach der Installation für die Ausführung vor.

   Wenn Sie Kaspersky Endpoint Security über die Befehlszeile installiert haben, starten Sie nach der Installation das Skript zur Erstkonfiguration oder führen Sie die Erstkonfiguration im automatischen Modus aus. Wählen Sie während der Erstkonfiguration den Light Agent-Modus auf eine der folgenden Arten aus:

   - Geben Sie im Skript für die Erstkonfiguration im Schritt `Specifying the application usage` den Wert `yes` ein.
   - Geben Sie in der Datei für die Erstkonfiguration den Parameter `KSVLA_MODE=yes` an.

   Wenn Sie Kaspersky Endpoint Security auf einer Vorlage installieren, aus der temporäre virtuelle Maschinen erstellt werden, wird empfohlen zusätzlich einen Parameter anzugeben, um die Ausführung auf temporären virtuellen Maschinen zu optimieren. Weitere Informationen über Installation virtueller Maschinen auf einer Vorlage finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

Installation und Erstkonfiguration des Administrationsagenten von Kaspersky Security Center

Um die Kaspersky Endpoint Security mithilfe von Kaspersky Security Center zu verwalten, müssen Sie den Administrationsagenten installieren.

Der Administrationsagent stellt die Kommunikation zwischen dem Client-Gerät und dem Administrationsserver von Kaspersky Security Center sicher. Daher muss er auf jedem Client-Gerät installiert werden, das mit dem zentralisierten Remote-Verwaltungssystem von Kaspersky Security Center verbunden wird.

Sie können die Installation und Erstkonfiguration des Administrationsagenten auf eine der folgenden Arten durchführen:

- per Fernzugriff vom Administrator-Arbeitsplatz aus über die Kaspersky Security Center Web Console oder über die Verwaltungskonsole;
- über die Befehlszeile.

Informationen zum Installieren des Administrationsagenten mithilfe von Kaspersky Security Center

Bevor Sie mit der Remote-Installation des Administrationsagenten mithilfe von Kaspersky Security Center beginnen, müssen Sie das Gerät für die Remote-Installation vorbereiten (siehe Hilfe zu Kaspersky Security Center, Abschnitt "Ein Linux-Gerät vorbereiten und den Administrationsagenten auf einem Linux-Gerät remote installieren").

Verwenden Sie für die Remote-Installation das Installationspaket des Administrationsagenten. Sie können die erforderlichen Dateie für die Erstellung des Installationspakets vom Administrationsagenten von der Kaspersky-Website im Abschnitt **Kaspersky Security Center** herunterladen.

So installieren Sie den Administrationsagenten aus der Ferne:

1. Erstellen Sie das Installationspaket für den Administrationsagenten.

   Während der Erstellung des Installationspakets müssen Sie die Bedingungen des Endbenutzer-Lizenzvertrags für den Administrationsagenten akzeptieren. Lesen Sie das Dokument "license.txt", das mit dem Administrationsagenten geliefert wurde, um sich mit dem Text des Endbenutzer-Lizenzvertrags vertraut zu machen.

   Geben Sie in den Einstellungen des Installationspakets die Adresse des Administrationsservers an, mit dem der Administrationsagent eine Verbindung herstellen soll, sowie den Port für die Verbindung.

2. Installieren Sie den Administrationsagenten mithilfe der Aufgabe zur Remote-Installation der App.

Weitere Informationen zur Installation des Administrationsagenten finden Sie in der Hilfe zu Kaspersky Security Center.

Informationen zum Installieren des Administrationsagenten über die Befehlszeile

Sie können den Administrationsagenten über die Befehlszeile auf eine der folgenden Arten installieren:

- Führen Sie die Installation und Erstkonfiguration im Silent-Modus mit einer Antwort-Datei durch. Eine Antwort-Datei ist eine Textdatei, die einen benutzerdefinierten Satz von Einstellungen für die Installation und Erstkonfiguration des Administrationsagenten enthält.

- Installieren Sie den Administrationsagenten aus einem Paket im RPM- oder DEB-Format entsprechend dem Typ des Paketmanagers und führen Sie dann die Erstkonfiguration des Administrationsagenten mithilfe eines Skripts im interaktiven Modus durch. Das Skript wird mit dem folgenden Befehl gestartet:

  - für ein 32-Bit-Betriebssystem:

    ```
    # /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl
    ```

  - für ein 64-Bit-Betriebssystem:

    ```
    # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
    ```

Die Installation des Administrationsagenten muss mit Root-Rechten gestartet werden.

So installieren Sie den Administrationsagenten im Silent-Modus:

1. Erstellen Sie eine Antwortdatei. Fügen Sie der Antwort-Datei eine Liste der Einstellungen für die Installation und Erstkonfiguration des Administrationsagenten im Format `< <Einstellung> >=< Wert >` hinzu, wobei jede Einstellung in einer separaten Zeile steht.

   Um die Antwort-Datei korrekt zu verwenden, müssen Sie die folgenden erforderlichen Einstellungen in die Datei einbinden:

   - KLNAGENT_SERVER – Vollqualifizierter Domänenname (FQDN) oder IP-Adresse des Administrationsservers.

   - KLNAGENT_AUTOINSTALL – Diese Einstellung bestimmt, ob die Installation im Silent-Modus durchgeführt wird oder nicht. Geben Sie den Wert `1` an.

   - EULA_ACCEPTED – Zustimmung zu den Bedingungen des Endbenutzer-Lizenzvertrags für den Administrationsagenten. Sie müssen die Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren, damit Sie mit dem Installationsprozess fortfahren können. Lesen Sie das Dokument "license.txt", das mit dem Administrationsagenten geliefert wurde, um sich mit dem Text des Endbenutzer-Lizenzvertrags vertraut zu

machen. Wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags verstehen und akzeptieren, geben Sie den Wert `1` an.

Sie können auch andere Einstellungen für die Installation und Erstkonfiguration des Administrationsagenten hinzufügen. Eine vollständige Liste der möglichen Einstellungen finden Sie in der Hilfe zu Kaspersky Security Center (Abschnitt "Administrationsagent für Linux im Silent-Modus installieren (mit einer Antwort-Datei)").

2. Legen Sie den Wert der Umgebungsvariablen KLAUTOANSWERS fest, indem Sie den vollständigen Namen der Antwort-Datei (einschließlich Pfad) eingeben, beispielsweise wie folgt:

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

3. Installieren Sie den Administrationsagenten:

   - Um den Administrationsagenten aus einem RPM-Paket auf einem 32-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:

     ```
     # rpm -i klnagent-<Build-Nummer>.i386.rpm
     ```

   - Um den Administrationsagenten aus einem RPM-Paket auf einem 64-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:

     ```
     # rpm -i klnagent64-<Build-Nummer>.x86_64.rpm
     ```

   - Um den Administrationsagenten aus einem RPM-Paket auf einem 64-Bit-Betriebssystem für Arm-Architektur zu installieren, führen Sie den folgenden Befehl aus:

     ```
     # rpm -i klnagent64-<Build-Nummer>.aarch64.rpm
     ```

   - Um den Administrationsagenten aus einem DEB-Paket auf einem 32-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:

     ```
     # apt-get install ./klnagent_<Build-Nummer>_i386.deb
     ```

   - Um den Administrationsagenten aus einem DEB-Paket auf einem 64-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:

     ```
     # apt-get install ./klnagent64_<Build-Nummer>_amd64.deb
     ```

   - Um den Administrationsagenten aus einem DEB-Paket auf einem 64-Bit-Betriebssystem für Arm-Architektur zu installieren, führen Sie den folgenden Befehl aus:

     ```
     # apt-get install ./klnagent64_<Build-Nummer>_arm64.deb
     ```

Verwaltungs-Plug-ins für Kaspersky Endpoint Security installieren

Zur Verwaltung der App Kaspersky Endpoint Security über Kaspersky Security Center müssen Sie das Verwaltungs-Plug-in für Kaspersky Endpoint Security installieren.

- Mit dem Web-Plug-in für die Verwaltung von Kaspersky Endpoint Security können Sie die App über die Kaspersky Security Center Cloud Console und die Kaspersky Security Center Web Console verwalten.

- Mit dem MMC-Plug-in für die Verwaltung von Kaspersky Endpoint Security können Sie die App über die Verwaltungskonsole von Kaspersky Security Center verwalten.

Sie können Verwaltungs-Plug-ins für mehrere Versionen der App Kaspersky Endpoint Security gleichzeitig installieren. Auf diese Weise können Sie die App unter Verwendung von Richtlinien verwalten, die mithilfe verschiedener Versionen des Verwaltungs-Plug-ins erstellt wurden.

Darüber hinaus können Richtlinien und Aufgaben, die mit älteren Versionen des Verwaltungs-Plug-ins erstellt wurden, zu neuen Versionen konvertiert werden.

Web-Plug-in für Kaspersky Endpoint Security installieren

Das Web-Plug-in für die Verwaltung von Kaspersky Endpoint Security muss auf dem Client-Gerät mit installierter App Kaspersky Security Center Web Console installiert werden. Die Funktionalität des Web-Plug-ins steht allen Administratoren zur Verfügung, die über einen Browser auf die Kaspersky Security Center Web Console zugreifen können.

Das Web-Plug-in kann wie folgt installiert werden:

- Mithilfe des Assistenten für die Erstkonfiguration von Kaspersky Security Center Web Console.

  Sobald Sie die Kaspersky Security Center Web Console zum ersten Mal mit dem Administrationsserver verbinden, schlägt die Kaspersky Security Center Web Console automatisch vor, den Assistenten für die Ersteinrichtung auszuführen. Sie können den Assistenten für die Ersteinrichtung auch in der Benutzeroberfläche der Kaspersky Security Center Web Console ausführen (**Gerätesuche und Softwareverteilung** → **Softwareverteilung und Zuweisung** → **Assistent für die Ersteinrichtung**). Der Assistent für die Erstkonfiguration kann auch überprüfen, ob die installierten Web-Plug-ins auf dem neuesten Stand sind und die erforderlichen Updates herunterladen. Weitere Informationen zum Assistenten für die Ersteinrichtung der Kaspersky Security Center Web Console finden Sie in der Hilfe zu Kaspersky Security Center.

- Manuell mithilfe eines Programmpakets aus der Liste der Web-Plug-ins von Kaspersky oder von einer externen Quelle.

So installieren Sie das Web-Plug-in für Kaspersky Endpoint Security manuell:

1. Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console **Einstellungen** → **Web-Plug-ins** aus.

   Die Liste der installierten Web-Plug-ins wird geöffnet.

2. Beginnen Sie mit der Installation des Web-Plug-ins für Kaspersky Endpoint Security auf eine der folgenden Arten:

   - Installation aus der Liste der Web-Plug-ins von Kaspersky:

     a. Klicken Sie auf **Hinzufügen**.

     Die Liste aller verfügbaren Web-Plug-ins von Kaspersky wird geöffnet. Die Liste wird automatisch aktualisiert, wenn neue Versionen der Web-Plug-ins veröffentlicht werden.

     b. Suchen Sie in der Liste das Web-Plug-in **Kaspersky Endpoint Security <Versionsnummer> für Linux** und klicken Sie auf den Namen.

     c. Klicken Sie im angezeigten Fenster mit einer Beschreibung des Web-Plug-ins auf die Schaltfläche **Plug-in installieren**.

     d. Warten Sie, bis die Installation abgeschlossen ist, und klicken Sie im Informationsfenster auf **OK**.

   - Installation des Web-Plug-ins von einer externen Quelle (Archive, die für die Installation von Web-Plug-ins erforderlich sind, sind im Paket enthalten):

     a. Klicken Sie auf **Aus Datei hinzufügen**.

b. Geben Sie im angezeigten Fenster den Pfad zum ZIP-Archiv mit dem Web-Plug-in-Programmpaket und den Pfad zur signierten Datei im TXT-Format an. Diese Datei befindet sich im Archiv mit dem Web-Plug-in.

c. Klicken Sie auf **Hinzufügen**.

d. Warten Sie, bis die Installation abgeschlossen ist, und klicken Sie im Informationsfenster auf **OK**.

Das neue Plug-in erscheint in der Liste der installierten Web-Plug-ins (**Einstellungen** → **Web-Plug-ins**).

Wenn Sie in den Eigenschaften des Administrationsservers von Kaspersky Security Center eine Sprache ausgewählt haben, die nicht in der Distribution der App Kaspersky Endpoint Security vorhanden ist, werden der Endbenutzer-Lizenzvertrag und die gesamte Benutzeroberfläche in der Kaspersky Security Center Web Console in englischer Sprache angezeigt.

MMC-Plug-in für Kaspersky Endpoint Security installieren

Das MMC-Plug-in für die Verwaltung von Kaspersky Endpoint Security muss auf jenem Client-Gerät installiert sein, auf dem auch die Verwaltungskonsole von Kaspersky Security Center installiert ist.

Vor der Installation des mm-Plug-ins für Kaspersky Endpoint Security müssen Sie sicherstellen, dass Kaspersky Security Center und Redist C ++ 2015 (Microsoft Visual C ++ 2015 Redistributable) installiert sind.

So installieren Sie das MMC-Plug-in:

Führen Sie auf dem Gerät, auf dem die Verwaltungskonsole von Kaspersky Security Center installiert ist, die ausführbare Datei klcfginst.msi aus.

Die Datei ist im Lieferumfang von Kaspersky Endpoint Security enthalten.

Nach der Installation wird das MMC-Verwaltungs-Plug-in in der Liste der installierten MMC-Verwaltungs-Plug-ins in den Eigenschaften des Administrationsservers von Kaspersky Security Center angezeigt.

So zeigen Sie die Liste der installierten MMC-Verwaltungs-Plug-ins an:

1. Wählen Sie in der Struktur der Kaspersky Security Center Verwaltungskonsole den Knoten **Administrationsserver <Name des Servers>** aus und öffnen Sie das Fenster mit den Eigenschaften des Administrationsservers auf eine der folgenden Arten:

   - über den Eintrag **Eigenschaften** im Kontextmenü des Knotens **Administrationsserver <Servername>**;
   - indem Sie auf den Link **Eigenschaften des Administrationsservers** klicken, der sich im Arbeitsbereich des Knotens **Administrationsserver <Servername>** im Block **Administrationsserver** befindet.

2. Wählen Sie in der Liste links im Abschnitt **Erweitert** den Abschnitt **Informationen zu installierten App-Verwaltungs-Plug-ins** aus.

   Im rechten Teil des Fensters wird in der Liste der installierten Verwaltungs-Plug-ins das MMC-Plug-in für die Verwaltung von Kaspersky Endpoint Security angezeigt: **Kaspersky Endpoint Security <Versionsnummer> für Linux**.

Installation und Erstkonfiguration der App mithilfe von Kaspersky Security Center

Sie können Kaspersky Endpoint Security per Fernzugriff vom Administrator-Arbeitsplatz aus über die Kaspersky Security Center Web Console oder über die Verwaltungskonsole auf dem Client-Gerät installieren.

Für die Remote-Installation wird ein Installationspaket für die App Kaspersky Endpoint Security verwendet. Das Installationspaket für Kaspersky Endpoint Security gilt für alle unterstützten Betriebssysteme und Typen der Prozessorarchitektur. Sie können ein Installationspaket über die Kaspersky Security Center Web Console oder über die Verwaltungskonsole erstellen.

Wenn Sie vorhaben, Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen zu verwenden (im Rahmen von Kaspersky Security for Virtualization Light Agent), müssen Sie die Einstellungen für die Erstkonfiguration der App in den Eigenschaften des Installationspakets (diese Methode ist nur in der Web Console verfügbar) oder in der Konfigurationsdatei autoinstall.ini (befindet sich im Installationspaket) konfigurieren.

Sie können die Kaspersky Endpoint Security im Unternehmensnetzwerk mithilfe verschiedener Methoden auf die Geräte verteilen.

Die Kaspersky Security Center Web Console unterstützt die folgenden Hauptszenarien der Bereitstellung:

- App mithilfe des Assistenten für die Bereitstellung des Schutzes installieren.
- App über die Aufgabe zur Remote-Installation der App installieren.

Die Kaspersky Security Center Verwaltungskonsole unterstützt die folgenden hauptsächlichen Bereitstellungsmethoden:

- App über den Assistenten für Remote-Installationen installieren.
- App über die Aufgabe zur Remote-Installation der App installieren.

Eine Beschreibung der Bereitstellungsmethoden finden Sie in der Hilfe zu Kaspersky Security Center.

Bei Bedarf können Sie das Protokoll der Remote-Installation der App mithilfe der Ferndiagnose von Client-Geräten von Kaspersky Security Center anzeigen.

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, wird weder die Programmaktivierung während der Installation noch die automatische Verteilung von Lizenzschlüsseln unterstützt. Kaspersky Endpoint Security erhält die Lizenzinformationen vom Schutzserver, nachdem eine Verbindung mit der SVM hergestellt wurde. Das separate Aktivieren von Kaspersky Endpoint Security ist nicht notwendig.

Nachdem die Installation der App mithilfe von Kaspersky Security Center abgeschlossen ist, müssen Sie die App für die Ausführung vorbereiten.

Um mithilfe von Kaspersky Security Center die Ausführung des auf den Geräten installierten Kaspersky Endpoint Security zu verwalten, müssen Sie diese Geräte in einer Administrationsgruppe platzieren. Sie können vor Beginn der Installation der App Kaspersky Endpoint Security in Kaspersky Security Center Administrationsgruppen anlegen, in die Sie die Geräte mit installierter App verschieben möchten, und Regeln für die automatische Verschiebung der Geräte in die Administrationsgruppen einrichten. Wenn keine Regeln zum Verschieben von Geräten in Administrationsgruppen konfiguriert sind, fügt Kaspersky Security Center alle Geräte, mit installiertem Administrationsagenten, die mit dem Administrationsserver verbunden sind, zur Liste **Nicht zugeordnete Geräte** hinzu. In diesem Fall müssen Sie die Geräte manuell in die Administrationsgruppen verschieben (Details finden Sie in der Hilfe zu Kaspersky Security Center).

Ein Installationspaket in der Web Console erstellen

In der Kaspersky Security Center Web Console können Sie ein Installationspaket auf eine der folgenden Arten erstellen:

- Aus einer Archivdatei, die Sie im Voraus vorbereitet haben.
- Aus einem Programmpaket, das auf Servern von Kaspersky gehostet wird.

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden möchten, müssen Sie die Einstellungen für die Erstkonfiguration der App in den Eigenschaften des erstellten Installationspakets auf der Registerkarte **Einstellungen** konfigurieren. Sie können die Einstellungen für die Erstkonfiguration auch mithilfe der Konfigurationsdatei konfigurieren, die im Installationspaket enthalten ist.

So bereiten Sie eine Archivdatei zum Erstellen eines Installationspakets vor:

1. Laden Sie das Archiv "kesl.zip" von der Download-Seite der Apps im Abschnitt **Kaspersky Endpoint Security für Linux** (**Weitere Programmpakete -> Files for Product remote installation**) herunter.
2. Entpacken Sie das Archiv "kesl.zip" in einen Ordner, auf den der Administrationsserver von Kaspersky Security Center zugreifen kann. Legen Sie im selben Ordner die Dateien der Distribution ab, die dem Typ des Betriebssystems, in dem Sie die App installieren möchten, und dem Typ des Paketmanagers entsprechen:
   - für die Installation von Kaspersky Endpoint Security:
     - kesl-12.1.0-<Build-Nummer>.i386.rpm (für 32-Bit-Betriebssysteme mit rpm)
     - kesl_12.1.0-<Build-Nummer>_i386.deb (für 32-Bit-Betriebssysteme mit dpkg)
     - kesl-12.1.0-<Build-Nummer>.x86_64.rpm (für 64-Bit-Betriebssysteme mit rpm)
     - kesl_12.1.0-<Build-Nummer>_amd64.deb (für 64-Bit-Betriebssysteme mit dpkg)
     - kesl-12.1.0-<Build-Nummer>.aarch64.rpm (für 64-Bit-Betriebssysteme für Arm-Architektur mit rpm)
     - kesl_12.1.0-<Build-Nummer>_arm64.deb (für 64-Bit-Betriebssysteme für Arm-Architektur mit dpkg)
   - für die Installation der grafischen Benutzeroberfläche:
     - kesl-gui-12.1.0-<Build-Nummer>.i386.rpm (für 32-Bit-Betriebssysteme mit rpm)
     - kesl-gui_12.1.0-<Build-Nummer>_i386.deb (für 32-Bit-Betriebssysteme mit dpkg)

- kesl-gui-12.1.0-<Build-Nummer>.x86_64.rpm (für 64-Bit-Betriebssysteme mit rpm)
- kesl-gui_12.1.0-<Build-Nummer>_amd64.deb (für 64-Bit-Betriebssysteme mit dpkg)
- kesl-gui-12.1.0-<Build-Nummer>.aarch64.rpm (für 64-Bit-Betriebssysteme für Arm-Architektur mit rpm)
- kesl-gui_12.1.0-<Build-Nummer>_arm64.deb (für 64-Bit-Betriebssysteme für Arm-Architektur mit dpkg)

Wenn Sie die grafische Benutzeroberfläche nicht installieren möchten, platzieren Sie diese Dateien nicht in dem Order, um die Größe des Installationspakets zu reduzieren.

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, wird die grafische Benutzeroberfläche nicht unterstützt.

Bitte beachten Sie, dass Sie bei Nichtverwendung der grafischen Benutzeroberfläche in den Eigenschaften des Installationspakets oder in der Konfigurationsdatei "autoinstall.ini" den Wert des entsprechenden Parameters mit `USE_GUI=No` festlegen müssen. Andernfalls wird die Installation mit einem Fehler beendet.

Wenn Sie mit dem zu erstellenden Installationspaket die App in Betriebssystemen oder Paketmanagern mehrerer Typen installieren möchten, platzieren Sie in diesem Ordner die Dateien für Betriebssysteme und Paketmanager aller erforderlichen Typen.

3. Wenn Sie die Einstellungen für die Erstkonfiguration der App mithilfe einer Konfigurationsdatei konfigurieren möchten, öffnen Sie die Konfigurationsdatei autoinstall.ini und geben Sie die erforderlichen Änderungen ein. Die Datei "autoinstall.ini" befindet sich in dem Ordner, in den Sie das Archiv "kesl.zip" extrahiert haben.

   Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen zu verwenden möchten, müssen Sie in der Konfigurationsdatei "autoinstall.ini" den Parameter `KSVLA_MODE=yes` festlegen.

   Sie können die Einstellungen für die Erstkonfiguration der App auch in den Eigenschaften des erstellten Installationspakets auf der Registerkarte **Einstellungen** konfigurieren.

4. Wenn Sie vorhaben, Kaspersky Endpoint Security im Standard-Modus zu verwenden und vorab heruntergeladene Datenbanken verwenden möchten, legen Sie die vorbereiteten Archive mit Datenbanken für alle erforderlichen Betriebssystemtypen in einem Ordner ab, öffnen Sie die Konfigurationsdatei autoinstall.ini und legen Sie den Wert des Parameters `UPDATE_EXECUTE=no` fest. Die Datei "autoinstall.ini" befindet sich in dem Ordner, in den Sie das Archiv "kesl.zip" extrahiert haben.

5. Legen Sie alle vorbereiteten Dateien in einem zip-, cap-, tar- oder tar.gz-Archiv unter einem beliebigen Namen ab.

So erstellen Sie ein Installationspaket für Kaspersky Endpoint Security in der Kaspersky Security Center Web Console:

1. Wählen Sie im Hauptfenster der Web Console einen der folgenden Abschnitte aus:
   - **Entdeckung und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete**.
   - **Vorgänge → Datenverwaltung → Installationspakete**.

Es öffnet sich eine Liste mit den verfügbaren Installationspaketen auf dem Administrationsserver.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Pakete wird gestartet. Folgen Sie den Anweisungen des Assistenten.

3. Wählen Sie auf der ersten Seite des Assistenten die Methode zum Erstellen des Installationspakets aus:

   - **Installationspaket aus einer Datei erstellen**. Das Installationspaket wird aus der Archivdatei erstellt, die Sie zuvor vorbereitet haben. Sie müssen diese Option auswählen, wenn Sie vorhaben, Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen zu verwenden.
   - **Installationspaket für eine Anwendung von Kaspersky erstellen**. Das Installationspaket wird aus einem Programmpaket erstellt, das auf den Servern von Kaspersky gehostet wird.

   In der Kaspersky Security Center Cloud Console können keine Installationspakete aus einer Datei erstellt werden.

4. Je nach gewählter Methode zum Erstellen eines Pakets:

   - Müssen Sie den Paketnamen angeben, auf die Schaltfläche **Durchsuchen** klicken und den Pfad zu dem Archiv angeben, das Sie zum Erstellen des Installationspakets vorbereitet haben.
   - Müssen Sie ein Programmpaket von Kaspersky Endpoint Security auswählen. Müssen Sie im rechten Fenster die Informationen zum Paket lesen und auf die Schaltfläche **Installationspaket herunterladen und erstellen** anklicken. Der Vorgang zur Erstellung des Installationspakets wird gestartet.

5. Während der Erstellung des Installationspakets müssen Sie die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie akzeptieren. Machen Sie sich nach Aufforderung des Assistenten mit dem Endbenutzer-Lizenzvertrag, der zwischen Ihnen und Kaspersky geschlossen wird, sowie mit der Datenschutzrichtlinie vertraut, in der die Verarbeitung und Übermittlung von Daten beschrieben wird. Um die Erstellung des Installationspakets fortzusetzen, müssen Sie bestätigen, dass Sie die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie vollständig gelesen haben und akzeptieren.

Das Installationspaket wird erstellt und der Liste mit Installationspaketen hinzugefügt. Mithilfe des Installationspakets können Sie die App auf Geräten im Unternehmensnetzwerk installieren oder die Version der App aktualisieren.

In den Einstellungen des Installationspakets können Sie auf der Registerkarte **Einstellungen** auch die Einstellungen für die Erstkonfiguration der App konfigurieren (s. Tabelle unten).

Die Konfiguration des Installationspakets von Kaspersky Endpoint Security wird erst ab Kaspersky Security Center Web Console Version 14.2 unterstützt. Verwenden Sie die Konfigurationsdatei autoinstall.ini, um die Einstellungen zu konfigurieren.

Einstellungen des Installationspakets

Abschnitt	Beschreibung
Angeben des Gebietsschemas	Aktivieren Sie das Kontrollkästchen, um das Gebietsschema festzulegen, das bei der Ausführung der App verwendet werden soll. Das Gebietsschema wird mittels RFC 3066-Format angegeben. Wenn diese Einstellung nicht angegeben wird, wird das Standard-Gebietsschema verwendet.
App aktivieren	Aktivieren Sie das Kontrollkästchen, um die App zu aktivieren. Sie können die App auch nach der Installation aktivieren.

	Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.
Auswählen der Update-Quelle	Geben Sie die Update-Quelle an: • **Kaspersky-Update-Server**. • **Kaspersky Security Center** • **Andere Quellen im lokalen oder globalen Netzwerk**. Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.
Starten der Update-Aufgabe nach der Installation	Aktivieren Sie das Kontrollkästchen, um nach der Installation der App die Update-Aufgabe auszuführen. Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.
Angeben der Proxy-Einstellungen	Aktivieren Sie dieses Kontrollkästchen, um die Adresse des Proxy-Servers anzugeben, der für die Verbindung zum Internet verwendet wird. Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.
Installieren des Kernel-Quellcodes	Aktivieren Sie dieses Kontrollkästchen, um die Kompilierung des Kernelmoduls automatisch zu starten.
Verwenden der grafischen Benutzeroberfläche	Aktivieren Sie dieses Kontrollkästchen, um die Verwendung der grafischen Benutzeroberfläche zu aktivieren. Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.
Angeben eines Benutzers mit Administratorrolle (admin)	Aktivieren Sie das Kontrollkästchen, um einen Benutzer anzugeben, dem die Administratorrolle (admin) zugewiesen werden soll.
Automatisches Konfigurieren von SELinux	Aktivieren Sie das Kontrollkästchen, um die automatische Konfiguration von SELinux für die Arbeit mit Kaspersky Endpoint Security auszuführen.
Benutzer aus privilegierten Gruppen löschen	Aktivieren Sie das Kontrollkästchen, um vor der Installation der App die Benutzer aus den privilegierten Gruppen "kesladmin" und "keslaudit" zu entfernen.

	Wenn das Kontrollkästchen aktiviert ist und die Gruppe "nogroup" nicht vorhanden ist, wird die Installation unterbrochen und Sie werden aufgefordert, die Benutzer manuell aus den privilegierten Gruppen zu entfernen.
Schutzkomponenten und Untersuchungsaufgaben beim ersten Start der App nach deren Installation deaktivieren	Aktivieren Sie das Kontrollkästchen, damit die App nach der Installation mit deaktivierten Schutzkomponenten und Untersuchungsaufgaben startet. Eine Installation mit deaktivierten Schutzkomponenten kann hilfreich sein, um beispielsweise ein Problem mit der App zu reproduzieren und eine Protokolldatei zu erstellen. Wenn Sie die erforderlichen Komponenten und Aufgaben aktivieren, wird die Ausführung der aktivierten Komponenten und Aufgaben nach einem Neustart der App fortgesetzt.
App im Light Agent-Modus verwenden	Aktivieren Sie das Kontrollkästchen, wenn Sie die App im Light Agent-Modus zum Schutz virtueller Umgebungen (im Rahmen von Kaspersky Security for Virtualization Light Agent) verwenden möchten. Wenn das Kontrollkästchen deaktiviert ist, wird die App im Standard-Modus verwendet.
Modus zum Schutz der VDI-Infrastruktur aktivieren	Aktivieren Sie das Kontrollkästchen, um den Modus zum Schutz der VDI-Infrastruktur zu aktivieren. Dies wird empfohlen, wenn die App auf einer Vorlage für virtuelle Maschinen installiert wird, aus der temporäre virtuelle Maschinen erstellt werden. Die Einstellung wird nur angewendet, wenn die App im Light Agent-Modus verwendet wird.
Geschützte virtuelle Maschine als Server verwenden	Aktivieren Sie das Kontrollkästchen, wenn die virtuelle Maschine, auf der die App installiert wird, als Server in der virtuellen Infrastruktur verwendet wird. Die Einstellung wird nur angewendet, wenn die App im Light Agent-Modus verwendet wird.

Ein Installationspaket in der Administrationskonsole erstellen

Bevor Sie ein Installationspaket für Kaspersky Endpoint Security erstellen, müssen Sie die Dateien vorbereiten, die im Paket enthalten sein sollen.

So bereiten Sie Dateien für die Erstellung eines Installationspakets vor:

1. Laden Sie das Archiv "kesl.zip" von der Download-Seite der Apps im Abschnitt **Kaspersky Endpoint Security für Linux** (**Weitere Programmpakete -> Files for Product remote installation**) herunter.

2. Entpacken Sie das Archiv "kesl.zip" in einen Ordner, auf den der Administrationsserver von Kaspersky Security Center zugreifen kann. Legen Sie im selben Ordner die Dateien der Distribution ab, die dem Typ des Betriebssystems, in dem Sie die App installieren möchten, und dem Typ des Paketmanagers entsprechen:

   - für die Installation von Kaspersky Endpoint Security:

- kesl-12.1.0-<Build-Nummer>.i386.rpm (für 32-Bit-Betriebssysteme mit rpm)
- kesl_12.1.0-<Build-Nummer>_i386.deb (für 32-Bit-Betriebssysteme mit dpkg)
- kesl-12.1.0-<Build-Nummer>.x86_64.rpm (für 64-Bit-Betriebssysteme mit rpm)
- kesl_12.1.0-<Build-Nummer>_amd64.deb (für 64-Bit-Betriebssysteme mit dpkg)
- kesl-12.1.0-<Build-Nummer>.aarch64.rpm (für 64-Bit-Betriebssysteme für Arm-Architektur mit rpm)
- kesl_12.1.0-<Build-Nummer>_arm64.deb (für 64-Bit-Betriebssysteme für Arm-Architektur mit dpkg)

- für die Installation der grafischen Benutzeroberfläche:
  - kesl-gui-12.1.0-<Build-Nummer>.i386.rpm (für 32-Bit-Betriebssysteme mit rpm)
  - kesl-gui_12.1.0-<Build-Nummer>_i386.deb (für 32-Bit-Betriebssysteme mit dpkg)
  - kesl-gui-12.1.0-<Build-Nummer>.x86_64.rpm (für 64-Bit-Betriebssysteme mit rpm)
  - kesl-gui_12.1.0-<Build-Nummer>_amd64.deb (für 64-Bit-Betriebssysteme mit dpkg)
  - kesl-gui-12.1.0-<Build-Nummer>.aarch64.rpm (für 64-Bit-Betriebssysteme für Arm-Architektur mit rpm)
  - kesl-gui_12.1.0-<Build-Nummer>_arm64.deb (für 64-Bit-Betriebssysteme für Arm-Architektur mit dpkg)

  Wenn Sie die grafische Benutzeroberfläche nicht installieren möchten, platzieren Sie diese Dateien nicht in dem Order, um die Größe des Installationspakets zu reduzieren.

  Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, wird die grafische Benutzeroberfläche nicht unterstützt.

Bitte beachten Sie, dass Sie bei Nichtverwendung der grafischen Benutzeroberfläche in den Eigenschaften des Installationspakets oder in der Konfigurationsdatei "autoinstall.ini" den Wert des entsprechenden Parameters mit `USE_GUI=No` festlegen müssen. Andernfalls wird die Installation mit einem Fehler beendet.

Wenn Sie mit dem zu erstellenden Installationspaket die App in Betriebssystemen oder Paketmanagern mehrerer Typen installieren möchten, platzieren Sie in diesem Ordner die Dateien für Betriebssysteme und Paketmanager aller erforderlichen Typen.

3. Wenn Sie die Einstellungen für die Erstkonfiguration der App mithilfe einer Konfigurationsdatei konfigurieren möchten, öffnen Sie die Konfigurationsdatei autoinstall.ini und geben Sie die erforderlichen Änderungen ein. Die Datei "autoinstall.ini" befindet sich in dem Ordner, in den Sie das Archiv "kesl.zip" extrahiert haben.

   Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen zu verwenden möchten, müssen Sie in der Konfigurationsdatei "autoinstall.ini" den Parameter `KSVLA_MODE=yes` festlegen.

4. Wenn Sie vorhaben, Kaspersky Endpoint Security im Standard-Modus zu verwenden und vorab heruntergeladene Datenbanken verwenden möchten, legen Sie die vorbereiteten Archive mit Datenbanken für alle erforderlichen Betriebssystemtypen in einem Ordner ab, öffnen Sie die Konfigurationsdatei autoinstall.ini

und legen Sie den Wert des Parameters `UPDATE_EXECUTE=no` fest. Die Datei "autoinstall.ini" befindet sich in dem Ordner, in den Sie das Archiv "kesl.zip" extrahiert haben.

So erstellen Sie ein Installationspaket für Kaspersky Endpoint Security in der Kaspersky Security Center Verwaltungskonsole:

1. Wählen Sie in der Konsolenstruktur den Punkt **Erweitert** → **Remote-Installation** → **Installationspakete** aus.
2. Klicken Sie auf die Schaltfläche **Installationspaket erstellen**.

   Der Assistent für neue Pakete wird gestartet.
3. Klicken Sie im Fenster des Assistenten auf die Schaltfläche **Installationspaket für das Kaspersky-Programm erstellen**.
4. Geben Sie den Namen des neuen Installationspakets ein und wechseln Sie zum nächsten Schritt.
5. Müssen Sie ein Programmpaket von Kaspersky Endpoint Security auswählen. Öffnen Sie dazu mit der Schaltfläche **Durchsuchen** ein Windows-Standardfenster und geben Sie den Pfad zur Datei "kesl.kud" an. Die Datei befindet sich in dem Ordner, in den Sie das Archiv "kesl.zip" extrahiert haben.

   Im Fenster wird der App-Name angezeigt.

   Wechseln Sie zum nächsten Schritt.
6. Machen Sie sich mit dem Endbenutzer-Lizenzvertrag, der zwischen Ihnen und Kaspersky geschlossen wird, sowie mit der Datenschutzrichtlinie vertraut, in der die Verarbeitung und Übermittlung von Daten beschrieben wird.

   Um die Erstellung des Installationspakets fortzusetzen, müssen Sie bestätigen, dass Sie die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie vollständig gelesen haben und akzeptieren. Aktivieren Sie im nächsten Fenster beide Kontrollkästchen, um zu bestätigen.

   Wechseln Sie zum nächsten Schritt.
7. Der Assistent lädt die Dateien, die für die Installation der App erforderlich sind, auf den Administrationsserver von Kaspersky Security Center herunter. Warten Sie, bis die Installation abgeschlossen ist.
8. Beenden Sie den Assistenten.

Das erstellte Installationspaket befindet sich im Strukturbaum der Verwaltungskonsole von Kaspersky Security Center im Ordner **Erweitert** → **Remote-Installation** → **Installationspakete**. Ein Installationspaket kann mehrmals verwendet werden.

Vorbereitung eines Archivs mit App-Datenbanken zur Erstellung eines Installationspakets mit integrierten Datenbanken

In einigen Fällen kann es notwendig sein, ein Remote-Installationspaket mit vorab heruntergeladenen App-Datenbanken erstellen. Beispielsweise, um die App auf einem Gerät mit Astra Linux Special Edition zu installieren, oder um die App sofort mit einsatzbereiten Datenbanken zu installieren (und somit ein späteres Aktualisieren der Datenbanken zu vermeiden).

So erstellen Sie ein Installationspaket mit integrierten Datenbanken zur App-Installation:

1. Installieren und konfigurieren Sie zunächst Kaspersky Endpoint Security mittels Befehlszeile oder mittels Kaspersky Security Center auf Ihrem Gerät.

2. Aktualisieren Sie die App-Datenbank. Für die Aktualisierung der Datenbanken während der Erstkonfiguration oder nach der Installation der App kann eine *Update*-Aufgabe auf folgende Arten gestartet werden: über die Befehlszeile, in der Kaspersky Security Center Verwaltungskonsole oder in der Kaspersky Security Center Web Console.

3. Kopieren Sie den Inhalt des Verzeichnisses "/var/opt/kaspersky/kesl/private/updates/" je nach Architektur des Betriebssystems, für das Sie ein Installationspaket mit integrierten Datenbanken erstellen, in eines der folgenden Unterverzeichnisse: "/i386/", "/ x86_64/" oder "/arm64/".

4. Platzieren Sie die Verzeichnisse mit Datenbanken im Archiv "kesl-bases.tgz" und behalten Sie dabei die Struktur der verschachtelten Verzeichnisse bei. Sie können entweder nur ein Unterverzeichnis mit Datenbanken für die gewünschte Betriebssystemarchitektur oder alle Unterverzeichnisse mit Datenbanken ("/i386/", "/x86_64/" oder "/arm64/") in einem Archiv für verschiedene Architekturen archivieren, wenn Sie vorhaben, ein Installationspaket für die Installation auf mehreren Betriebssystemen mit unterschiedlichen Architekturen zu erstellen.

5. Sie können das erstellte Archiv mit den App-Datenbanken verwenden, wenn Sie in der Kaspersky Security Center Verwaltungskonsole oder in der Kaspersky Security Center Web Console ein Installationspaket erstellen.

Parameter der Konfigurationsdatei "autoinstall.ini"

In der Konfigurationsdatei "autoinstall.ini" können Sie die in der folgenden Tabelle aufgeführten Parameter festlegen. Der Umfang der anwendbaren Einstellungen, hängt dabei vom Nutzungsmodus der App ab.

Parameter der Konfigurationsdatei "autoinstall.ini"

Einstellung	Beschreibung	Werte
KSVLA_MODE	Nutzungsmodus von Kaspersky Endpoint Security.	`yes` – Kaspersky Endpoint Security wird im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet (im Rahmen von Kaspersky Security for Virtualization Light Agent). `no` (Standardwert) – Kaspersky Endpoint Security wird im Standard-Modus verwendet.
SERVER_MODE	Rolle der geschützten virtuellen Maschine (Server oder Workstation). Die Einstellung wird nur angewendet, wenn die App im Light Agent-Modus verwendet wird.	`yes` (Standardwert) – die geschützte virtuelle Maschine wird als Server verwendet. `no` – Die geschützte virtuelle Maschine wird als Workstation verwendet.
VDI_MODE	Aktivieren des Modus zum Schutz der VDI-Infrastruktur, um die Leistung der App auf temporären virtuellen Maschinen zu optimieren.	`yes` – Modus zum Schutz der VDI-Infrastruktur aktivieren. Dies wird empfohlen, wenn Kaspersky Endpoint Security auf einer Vorlage für virtuelle Maschinen installiert ist, aus der temporäre virtuelle Maschinen erstellt werden.

	Die Einstellung wird nur angewendet, wenn die App im Light Agent-Modus verwendet wird.	no (Standardwert) – Modus zum Schutz der VDI-Infrastruktur nicht aktivieren.
EULA_AGREED	Erforderliche Einstellung. Annahme der Bedingungen des Endbenutzer-Lizenzvertrags.	yes (Standardwert) – Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren, um den Installationsprozess der App fortzusetzen. no – Bedingungen des Endbenutzer-Lizenzvertrags nicht akzeptieren. Die Installation der App wird abgebrochen.
PRIVACY_POLICY_AGREED	Erforderliche Einstellung. Zustimmung zu den Bedingungen der Datenschutzrichtlinie.	yes (Standardwert) – Bedingungen der Datenschutzrichtlinie akzeptieren, um den Installationsprozess der App fortzusetzen. no – Bedingungen der Datenschutzrichtlinie nicht akzeptieren. Die Installation der App wird abgebrochen.
USE_KSN	Erforderliche Einstellung. Verwendung von Kaspersky Security Network aktivieren. Um die Nutzung von KSN zu aktivieren, müssen Sie die Bedingungen der Erklärung zu Kaspersky Security Network akzeptieren.	yes – Bedingungen der Erklärung zu Kaspersky Security Network-akzeptieren und die Verwendung von KSN aktivieren. no (Standardwert) – Bedingungen der Erklärung zu Kaspersky Security Network nicht akzeptieren. Wenn Kaspersky Endpoint Security im Standard-Modus verwendet wird und Sie die Verwendung von KSN aktiviert haben, wird automatisch der Cloud-Modus der App aktiviert. In diesem Modus verwendet Kaspersky Endpoint Security eine schlankere Version der Malware-Datenbanken.
GROUP_CLEAN	Erforderliche Einstellung. Entfernen von Benutzern aus den privilegierten Gruppen "kesladmin" und "keslaudit".	yes – Die Benutzer werden aus den privilegierten Gruppen entfernt. Wenn der Wert yes angegeben wurden und die Gruppe "nogroup" nicht vorhanden ist, wird die Installation unterbrochen und werden Sie aufgefordert, die Benutzer manuell aus den privilegierten Gruppen zu entfernen. no – Die Benutzer werden nicht aus den privilegierten Gruppen entfernen.
LOCALE	Optionale Einstellung.	Das Gebietsschema wird mittels RFC 3066-Format angegeben.

	Gebietsschema, das für die Lokalisierung von Ereignissen in der App verwendet wird, die an Kaspersky Security Center gesendet werden.	Wird die Einstellung `LOCALE` nicht angegeben, so wird das Gebietsschema des Betriebssystems verwendet. Wenn die App keine Sprachversion des Betriebssystems bestimmen konnte oder das Betriebssystem diese Lokalisierung nicht unterstützt, wird standardmäßig `en_US.utf8` installiert. Die Lokalisierung der grafischen Benutzeroberfläche und der Befehlszeile der App hängt von der Lokalisierung ab, die in der Umgebungsvariablen `LANG` angegeben ist. Wenn in der Umgebungsvariablen `LANG` eine Lokalisierung angegeben ist, die von der App Kaspersky Endpoint Security nicht unterstützt wird, werden die grafische Benutzeroberfläche und die Befehlszeile in der englischen Lokalisierung angezeigt.
INSTALL_LICENSE	Aktivierungscode oder Schlüsseldatei Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.	
UPDATER_SOURCE	Update-Quelle Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.	`SCServer` – Administrationsserver von Kaspersky Security Center als Update-Quelle verwenden `KLServers` – die Kaspersky-Update-Server als Update-Quelle verwenden Dieser Wert wird standardmäßig verwendet. Adresse der Update-Quelle
PROXY_SERVER	Adresse des Proxy-Servers, der für die Internetverbindung verwendet wird Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.	Adresse des Proxy-Servers
UPDATE_EXECUTE	Aufgabe zum Update der App-Datenbanken während des Konfigurationsvorgangs starten	`yes` (Standardwert) – Update-Aufgabe starten. `no` – Update-Aufgabe nicht starten

	Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.	
KERNEL_SRCS_INSTALL	Automatischer Start der Kompilierung des Kernelmoduls	`yes` (Standardwert) – Kernel-Modul kompilieren `no` – Kernel-Modul nicht kompilieren
USE_GUI	Verwendung des Pakets mit der grafischen Benutzeroberfläche. Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.	`yes` – Verwendung der grafischen Benutzeroberfläche aktivieren. `no` (Standardwert) – Verwendung der grafischen Benutzeroberfläche deaktivieren.
ADMIN_USER	Benutzer, dem die Administratorrolle (admin) zugewiesen ist.	Nein
CONFIGURE_SELINUX	Automatische Konfiguration von SELinux für die Arbeit mit der App Kaspersky Endpoint Security.	`yes` (Standardwert) – Automatische Konfiguration von SELinux für die Arbeit mit Kaspersky Endpoint Security ausführen. `no` – Automatische Konfiguration von SELinux für die Arbeit mit Kaspersky Endpoint Security nicht ausführen.
DISABLE_PROTECTION	Deaktivieren funktionaler Komponenten der App nach deren Installation. Eine Installation mit deaktivierten Komponenten kann hilfreich sein, um beispielsweise ein Problem mit der App zu reproduzieren und eine Protokolldatei zu erstellen. Wenn Sie nach der Installation der App mit dem Parameter `DISABLE_PROTECTION=yes` die erforderlichen Komponenten und Aufgaben aktivieren, werden die aktivierten Komponenten und Aufgaben nach einem Neustart der App ausgeführt.	`yes` – Schutzkomponenten und Untersuchungsaufgaben beim ersten Start der App nach deren Installation deaktivieren. `no` – Schutzkomponenten und Untersuchungsaufgaben beim ersten Start der App nach deren Installation nicht deaktivieren.
DISABLE_FILEAV_ACTIONS	Deaktivieren der Desinfektions- und Dateilöschfunktionen für Komponenten der App, nachdem sie installiert wurde.	`yes` – Desinfektions- und Dateilöschfunktionen beim Starten der App nach der Installation deaktivieren.

	Wenn die Desinfektions- und Dateilöschfunktionen deaktiviert sind und eine Bedrohung erkannt wird, versucht die App nicht, die Dateien mit der erkannten Bedrohung zu desinfizieren oder zu löschen. Stattdessen informiert sie den Benutzer lediglich darüber, dass in den Dateien eine Bedrohung erkannt wurde. Nach der Installation der App können Sie die Funktionen zum Desinfizieren und Löschen von Dateien mithilfe des Parameters `DisableFileAvActions` in der Konfigurationsdatei kesl.ini aktivieren.	`no` (Standardwert) – Desinfektions- und Dateilöschfunktionen beim Starten der App nach der Installation nicht deaktivieren.

Wenn Sie die Einstellungen in der Konfigurationsdatei autonistall.ini ändern möchten, geben Sie die Werte für die Einstellungen im Format <Name der Einstellung>=<Einstellungswert> ein (die App verarbeitet keine Leerzeichen zwischen dem Namen der Einstellung und ihrem Wert).

App für die gemeinsame Ausführung mit Kaspersky Security Center vorbereiten

Nach der Bereitstellung von Kaspersky Endpoint Security mittels Kaspersky Security Center müssen Sie die App auf deren Ausführung vorbereiten. Die durchzuführenden Maßnahmen hängen von dem Modus ab, in dem Sie Kaspersky Endpoint Security verwenden möchten.

Standard-Modus

Wenn Sie Kaspersky Endpoint Security im Standard-Modus verwenden möchten, müssen Sie nach der Bereitstellung der App die folgenden Maßnahmen durchführen:

- App aktivieren. Sie können die Aktivierungsaufgabe über die Verwaltungskonsole oder über die Kaspersky Security Center Web Console erstellen und ausführen sowie den Lizenzschlüssel aus dem Schlüsselspeicher von Kaspersky Security Center verteilen.
- Datenbanken und Module der App über die Verwaltungskonsole oder über die Kaspersky Security Center Web Console aktualisieren. Sie können die *Update-Aufgabe* verwenden, die automatisch vom Assistenten bei der Ersteinrichtung von Kaspersky Security Center nach der Installation des MMC-Verwaltungs-Plug-ins oder des Web-Plug-ins zur Verwaltung von Kaspersky Endpoint Security erstellt wird.
- Konfigurieren Sie eine Richtlinie, um die App mithilfe der Kaspersky Security Center Verwaltungskonsole der Web Console zentral Verwalten zu können. Sie können die Richtlinie verwenden, die automatisch vom Assistenten bei der Ersteinrichtung von Kaspersky Security Center nach der Installation des MMC-Verwaltungs-Plug-ins oder des Web-Plug-ins zur Verwaltung von Kaspersky Endpoint Security erstellt wird.

  Sie können auch Aufgaben zur Verwaltung der App mithilfe der Verwaltungskonsole oder Web Console konfigurieren.

Light Agent-Modus

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Infrastrukturen verwenden möchten, müssen Sie nach der Bereitstellung der App die folgenden Maßnahmen durchführen:

1. Konfigurieren Sie Einstellungen der SVM-Erkennung durch die Light Agents. Dies benötigt die Erstellung und Konfiguration einer Richtlinie für die zentralisierte Verwaltung der App-Ausführung auf den Client-Geräten. Für die Arbeit mit der Richtlinie können Sie die Verwaltungskonsole oder die Web Console verwenden.

   In den Eigenschaften der Richtlinie müssen Sie die folgenden Einstellungen konfigurieren:

   - Parameter für die Verbindung von Light Agents zum Integrationsserver.
   - Parameter für die Verbindung von Light Agents zur SVM.

2. Stellen Sie sicher, eine Verbindung zwischen den Light Agents und der SVM bzw. dem Integrationsserver besteht.

   Sie können die Verbindungsinformationen mithilfe der Befehle von Kaspersky Endpoint Security auf einer geschützten virtuellen Maschine abrufen:

   - Informationen über die Verbindung zur SVM können Sie mit folgendem Befehl abrufen: `kesl-control [-V] --svm-info`.
   - Informationen über die Verbindung zum Integrationsserver können Sie mit folgendem Befehl abrufen: `kesl-control [-V] --viis-info`.

3. Wenn Sie Kaspersky Endpoint Security als Light Agent verwenden, stellen Sie sicher, dass es Informationen über jene Lizenz abrufen kann, unter der Kaspersky Security for Virtualization Light Agent aktiviert ist.

   Nach der Aktivierung der Lösung auf den SVMs und der Verbindung der Light Agents mit den SVMs übermittelt der Schutzserver die Lizenzinformationen an die Light Agents. Informationen über die Lizenz, die Kaspersky Endpoint Security als Teil der Lösung verwendet, können Sie auf einer geschützten virtuellen Maschine mit folgendem Befehl anzeigen: `kesl-control -L --query`

4. Stellen Sie sicher, dass auf den geschützten virtuellen Maschinen die zur Ausführung des Light Agent erforderlichen Datenbankaktualisierungen installiert sind.

   Die Datenbanken auf geschützten virtuellen Maschinen werden mithilfe einer speziellen *Update*-Aufgabe aktualisiert, bei welcher der Ordner auf der SVM als Update-Quelle angegeben wird. Diese Update-Aufgabe wird automatisch gestartet.

   Auf einer geschützten virtuellen Maschine mit Light Agent können Sie die Aktualität der Datenbanken mit folgendem Befehl überprüfen: `kesl-control --app-info`.

   Sie können auch Aufgaben zur Verwaltung der App mithilfe der Verwaltungskonsole oder Web Console konfigurieren.

App mithilfe von Kaspersky Security Center aktivieren

Aktivierung – Vorgang, bei dem die App durch eine Lizenz aktiviert wird, die die Nutzung der Vollversion der App während der Gültigkeitsdauer der Lizenz ermöglicht.

Wenn Sie vorhaben, Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen zu verwenden, muss die App nach ihrer Installation nicht aktiviert werden. Sie aktivieren Kaspersky Security for Virtualization Light Agent und die Aktivierung erfolgt auf der Seite des Schutzservers (dies ist eine Komponente von Kaspersky Security for Virtualization Light Agent). Weitere Informationen finden Sie in der Hilfe von Kaspersky Security for Virtualization Light Agent.

Das Verfahren zur Aktivierung von Kaspersky Endpoint Security umfasst das Hinzufügen des Lizenzschlüssels der App.

Wenn Sie die App unter einer Lizenz verwenden, welche die Funktionalität von Kaspersky Endpoint Detection and Response Optimum nicht abdeckt, müssen Sie zur Aktivierung dieser Funktionalität einen zusätzlichen Lizenzschlüssel für das Add-on von Kaspersky Endpoint Detection and Response Optimum hinzufügen (im Weiteren auch "EDR Optimum-Schlüssel").

Sie können der App auf folgende Arten Lizenzschlüssel über Kaspersky Security Center hinzufügen:

- Durch Verwendung der Aufgabe für das Hinzufügen eines Schlüssels zur App

  Mittels dieser Methode können Sie einen Lizenzschlüssel zum jeweiligen Gerät oder zu Geräten hinzufügen, die zur Administrationsgruppe gehören. Sie können die Aufgabe zum Hinzufügen eines Schlüssels über die Web Console von Kaspersky Security Center oder über die Verwaltungskonsole erstellen und ausführen.

- Durch Verteilung eines Lizenzschlüssels, der sich auf dem Administrationsserver von Kaspersky Security Center befindet, auf die Client-Geräte.

  Mithilfe dieser Methode können Sie den Schlüssel automatisch zu Client-Geräten hinzufügen, die bereits mit Kaspersky Security Center verbunden sind, sowie zu neuen Client-Geräten hinzufügen. Um diese Methode nutzen zu können, müssen Sie den Schlüssel zunächst dem Schlüsselspeicher des Administrationsservers von Kaspersky Security Center hinzufügen.

- Dies geschieht durch das Hinzufügen eines Schlüssels zum Installationspaket von Kaspersky Endpoint Security.

  Mit dieser Methode können Sie bei der Bereitstellung von Kaspersky Endpoint Security den Schlüssel zu den Eigenschaften des Installationspakets hinzufügen. Die App wird nach der Installation automatisch aktiviert.

Um Aufgaben für das Hinzufügen des Schlüssels zur App, für das Hinzufügen des Schlüssels zum Schlüsselspeicher und für die Verteilung des Schlüssels auf Client-Geräten zu erstellen, können Sie die Verwaltungskonsole von Kaspersky Security Center oder die Kaspersky Security Center Web Console verwenden.

Aktivierung in der Kaspersky Security Center Web Console

Vor der Erstellung einer Aufgabe für das Hinzufügen eines Schlüssels zur App oder Verteilung des Schlüssels muss der Schlüssel zur Datenverwaltung des Administrationsservers von Kaspersky Security Center hinzugefügt werden.

So fügen Sie mithilfe der Web Console den Schlüssel zum Schlüsselspeicher von Kaspersky Security Center hinzu:

1. Wählen Sie im Hauptfenster von Web Console die Option **Vorgänge → Lizenzen für Kaspersky-Software**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie im nächsten Fenster eine Methode für das Hinzufügen des Schlüssels zum Speicher aus:
   - **Aktivierungscode eingeben**, wenn Sie einen Schlüssel mithilfe eines Aktivierungscodes hinzufügen möchten.

- **Schlüsseldatei hinzufügen**, wenn Sie einen Schlüssel mithilfe einer Schlüsseldatei hinzufügen möchten.

4. Führen Sie abhängig davon, welche Methode zum Hinzufügen des Schlüssels Sie im vorherigen Schritt ausgewählt haben, eine der folgenden Aktionen aus:

   - Geben Sie den Aktivierungscode ein und klicken Sie auf **Senden**.
   - Klicken Sie auf die Schaltfläche **Wählen Sie die Schlüsseldatei** und wählen Sie im folgenden Fenster eine Schlüsseldatei mit der Erweiterung "key" aus.

5. Klicken Sie auf **Schließen**.

Der hinzugefügte Schlüssel wird in der Liste mit Schlüsseln angezeigt.

So fügen Sie der App über die Web Console einen Schlüssel hinzu, indem Sie die Aufgabe zum Hinzufügen eines Schlüssels verwenden:

1. Wählen Sie im Hauptfenster der Web Console die Option **Assets (Geräte)** → **Aufgaben**.

   Die Liste mit Aufgaben wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Konfigurieren Sie die Aufgabeneinstellungen:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** den App-Namen Kaspersky Endpoint Security aus.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Schlüssel hinzufügen**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, z. B. `Kaspersky Endpoint Security aktivieren`.

   d. Wählen Sie im Abschnitt **Geräte, denen die Aufgabe zugewiesen wird** den Gültigkeitsbereich der Aufgabe aus. Klicken Sie auf **Weiter**.

4. Wählen Sie die Geräte entsprechend der Option für den ausgewählten Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.

   Das Fenster **Schlüsselspeicher von Kaspersky Security Center** wird geöffnet.

5. Wenn Sie bereits einen Schlüssel zum Schlüsselspeicher von Kaspersky Security Center hinzugefügt haben, wählen Sie den Schlüssel in der Liste aus und klicken Sie auf **Weiter**.

6. Wenn sich der erforderliche Schlüssel nicht im Schlüsselspeicher befindet, klicken Sie auf die Schaltfläche **Schlüssel hinzufügen**.

   a. Wählen Sie im nächsten Fenster eine Methode für das Hinzufügen des Schlüssels zum Speicher aus:

      - **Aktivierungscode eingeben**, wenn Sie einen Schlüssel mithilfe eines Aktivierungscodes hinzufügen möchten.
      - **Schlüsseldatei hinzufügen**, wenn Sie einen Schlüssel mithilfe einer Schlüsseldatei hinzufügen möchten.

   b. Führen Sie abhängig davon, welche Methode zum Hinzufügen des Schlüssels Sie im vorherigen Schritt ausgewählt haben, eine der folgenden Aktionen aus:

- Geben Sie den Aktivierungscode ein und klicken Sie auf **Senden**.
- Klicken Sie auf die Schaltfläche **Wählen Sie die Schlüsseldatei** und wählen Sie im folgenden Fenster eine Schlüsseldatei mit der Erweiterung "key" aus.

c. Lesen Sie die Informationen zum Schlüssel und klicken Sie auf die Schaltfläche **Schließen**.

d. Der hinzugefügte Schlüssel wird in der Liste mit Schlüsseln angezeigt. Wählen Sie ihn in der Liste aus und klicken Sie auf **Weiter**.

7. Lesen Sie die Lizenzinformationen und klicken Sie auf die Schaltfläche **Weiter**.
8. Beenden Sie den Assistenten.

   Eine neue Aufgabe wird in der Liste mit Aufgaben angezeigt.
9. Aktivieren Sie das Kontrollkästchen neben der Aufgabe. Klicken Sie auf die Schaltfläche **Ausführen**.

In den Eigenschaften der Aufgabe *Schlüssel hinzufügen* können Sie einen *Reserveschlüssel* zum Gerät hinzufügen. Der Reserveschlüssel wird aktiv, sobald die an den aktiven Schlüssel gebundene gültige Lizenz abläuft oder der aktive Schlüssel gelöscht wird. Ein Reserveschlüssel verhindert, dass nach Ablauf der Lizenz die Funktionalität der App eingeschränkt wird.

Wenn Sie einen Reserveschlüssel hinzufügen und die App noch keinen aktiven Schlüssel besitzt schlägt die Aufgabe fehl.

So fügen Sie der App in der Web Console einen Schlüssle hinzu, indem Sie die Verteilung eines Schlüssels vom Administrationsserver an die Geräte verwenden:

1. Wählen Sie im Hauptfenster von Web Console die Option **Vorgänge → Lizenzen für Kaspersky-Software**.
2. Öffnen Sie die Schlüssel-Einstellungen über den Link mit dem Namen der App, für deren Aktivierung der Schlüssel vorgesehen ist.
3. Aktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.
4. Klicken Sie auf **Speichern**.

   Der Lizenzschlüssel wird automatisch an die entsprechenden Client-Geräte verteilt. Bei der automatischen Verteilung des Schlüssels als aktiver Schlüssel oder Reserveschlüssel werden die Lizenzbeschränkungen nach Anzahl der Geräte (wie in den Schlüssel-Einstellungen festgelegt) berücksichtigt. Wenn die Lizenzbeschränkung erreicht ist, wird die Verteilung des Schlüssels an die Geräte automatisch beendet. Die Anzahl der Geräte auf denen der Schlüssel hinzugefügt wurde, sowie andere Daten finden sie in den Schlüssel-Einstellungen auf der Registerkarte **Geräte**.

In der Kaspersky Security Center Web Console können Sie die Verwendung der Lizenzen auf folgende Arten kontrollieren:

- Durch Anzeigen des Berichts über die Nutzung von Lizenzschlüsseln (**Überwachung und Berichterstattung → Berichte**).
- Durch Anzeigen der Statuswerte der verwalteten Geräte (**Assets (Geräte) → Verwaltete Geräte**). Wenn die App nicht aktiviert ist, werden für Geräte der Status und die Statusbeschreibung **Schutz deaktiviert** angezeigt.

- Durch Anzeigen der Schlüssel-Einstellungen (**Vorgänge** → **Lizenzen von Kaspersky**).

Besonderheiten bei der Aktivierung in Kaspersky Security Center Cloud Console

Für die Kaspersky Security Center Cloud Console ist eine Testversion verfügbar. *Testversion* – Eine spezielle Version der Kaspersky Security Center Cloud Console, mit der Benutzer die Funktionen von Kaspersky Security Center Cloud Console kennenlernen können. In dieser Version können Sie über einen Zeitraum von 30 Tagen Aktionen in einem Arbeitsbereich ausführen. Alle verwalteten Apps einschließlich der App Kaspersky Endpoint Security werden automatisch unter der Testlizenz der Kaspersky Security Center Cloud Console aktiviert. Es ist nicht möglich, die App Kaspersky Endpoint Security mit einer eigenen Testlizenz zu aktivieren, sobald die Testlizenz für Kaspersky Security Center Cloud Console abläuft. Nähere Informationen zur Kaspersky Security Center Cloud Console finden Sie in der Dokumentation zur Kaspersky Security Center Cloud Console.

Es ist nicht möglich, im Anschluss an die Verwendung der Testversion der Kaspersky Security Center Cloud Console zu einer kommerziellen Version zu wechseln. Alle Arbeitsbereiche der Testversion werden nach Ablauf des 30-tägigen Zeitraums automatisch samt allen Inhalten gelöscht.

Installation und Erstkonfiguration der App über die Befehlszeile

Bei der Installation einer App über die Befehlszeile können Sie folgende Aktionen ausführen:

- App mit grafischer Benutzeroberfläche installieren.

  Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird (im Rahmen von Kaspersky Security for Virtualization Light Agent), wird die grafische Benutzeroberfläche nicht unterstützt. Sie müssen das App-Paket ohne die grafische Benutzeroberfläche installieren.

- App ohne grafische Benutzeroberfläche installieren.
- Grafische Benutzeroberfläche auf dem Gerät installieren, auf dem die App installiert ist.

  Es ist nicht möglich, die grafische Benutzeroberfläche auf einem Gerät zu installieren, auf dem die App nicht installiert ist.

Wenn die Version des apt-Paketmanagers älter ist als 1.1.X, muss je nach Betriebssystem der dpkg- bzw. rpm-Paketmanager für die Installation verwendet werden.

Nach Abschluss der App-Installation muss eine Erstkonfiguration der App im interaktiven Modus oder im automatischen Modus vorgenommen werden.

App über die Befehlszeile installieren

App ohne grafische Benutzeroberfläche installieren

Um Kaspersky Endpoint Security aus einem Paket im RPM-Format auf einem 32-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:

```
# rpm -i kesl-12.1.0-<Build-Nummer>.i386.rpm
```

Um Kaspersky Endpoint Security aus einem Paket im RPM-Format auf einem 64-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:

```
# rpm -i kesl-12.1.0-<Build-Nummer>.x86_64.rpm
```

Um Kaspersky Endpoint Security aus einem Paket im RPM-Format auf einem 64-Bit-Betriebssystem für Arm-Architektur zu installieren, führen Sie den folgenden Befehl aus:

```
# rpm -i kesl-12.1.0-<Build-Nummer>.aarch64.rpm
```

Um Kaspersky Endpoint Security aus einem Paket im DEB-Format auf einem 32-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:

```
# apt-get install ./kesl_12.1.0-<Build-Nummer>_i386.deb
```

Um Kaspersky Endpoint Security aus einem Paket im DEB-Format auf einem 64-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:

```
# apt-get install ./kesl_12.1.0-<Build-Nummer>_amd64.deb
```

Um Kaspersky Endpoint Security aus einem Paket im DEB-Format auf einem 64-Bit-Betriebssystem für Arm-Architektur zu installieren, führen Sie den folgenden Befehl aus:

```
# apt-get install ./kesl_12.1.0-<Build-Nummer>_arm64.deb
```

Grafische Benutzeroberfläche installieren

Um die grafische Benutzeroberfläche aus einem Paket im rpm-Format auf einem 32-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:

```
# rpm -i kesl-gui-12.1.0-<Build-Nummer>.i386.rpm
```

Um die grafische Benutzeroberfläche aus einem Paket im rpm-Format auf einem 64-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:

```
# rpm -i kesl-gui-12.1.0-<Build-Nummer>.x86_64.rpm
```

Um die grafische Benutzeroberfläche aus einem Paket im RPM-Format auf einem 64-Bit-Betriebssystem für Arm-Architektur zu installieren, führen Sie den folgenden Befehl aus:

```
# rpm -i kesl-gui-12.1.0-<Build-Nummer>.aarch64.rpm
```

Um die grafische Benutzeroberfläche aus einem Paket im DEB-Format auf einem 32-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:

```
# apt-get install ./kesl-gui_12.1.0-<Build-Nummer>_i386.deb
```

Um die grafische Benutzeroberfläche aus einem Paket im DEB-Format auf einem 64-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:

```
# apt-get install ./kesl-gui_12.1.0-<Build-Nummer>_amd64.deb
```

Um die grafische Benutzeroberfläche aus einem Paket im DEB-Format auf einem 64-Bit-Betriebssystem für Arm-Architektur zu installieren, führen Sie den folgenden Befehl aus:

```
# apt-get install ./kesl-gui_12.1.0-<Build-Nummer>_arm64.deb
```

Ersteinrichtung der App im interaktiven Modus

Nach der Installation der App Kaspersky Endpoint Security mithilfe der Befehlszeile muss eine Erstkonfiguration der App durchgeführt werden. Starten Sie dazu das Skript zur Erstkonfiguration. Das Skript zur Erstkonfiguration ist im Lieferumfang von Kaspersky Endpoint Security enthalten.

Die Durchführung der Erstkonfiguration nach der Installation der App mithilfe der Befehlszeile ist erforderlich, um den Schutz der Client-Geräte zu aktivieren.

Um das Skript zur Erstkonfiguration von Kaspersky Endpoint Security zu starten, führen Sie den folgenden Befehl aus:

```
# /opt/kaspersky/kesl/bin/kesl-setup.pl
```

Das Skript zur Erstkonfiguration muss nach Abschluss der Installation des Kaspersky Endpoint Security-Pakets mit Root-Rechten ausgeführt werden. Das Skript fordert die Einstellungswerte von Kaspersky Endpoint Security schrittweise an. Sobald das Skript abgeschlossen ist und die Befehlszeile freigegeben wird, ist der Prozess der Erstkonfiguration der App beendet.

Um den Rückgabe-Code zu prüfen, führen Sie den folgenden Befehl aus:

```
echo $?
```

Wenn der Code 0 zurückgegeben wird, ist die Erstkonfiguration der App erfolgreich abgeschlossen.

Nutzungsmodus auswählen

Wählen Sie in diesem Schritt den Nutzungsmodus für Kaspersky Endpoint Security aus.

- Geben Sie `yes` ein, wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen nutzen möchten.
- Geben Sie `no` ein, wenn Sie Kaspersky Endpoint Security im Standard-Modus verwenden möchten.

Nachdem die Ersteinrichtung abgeschlossen ist, können Sie den Nutzungsmodus der App nicht mehr ändern.

Rolle der virtuellen Maschine festlegen

Dieser Schritt wird nur angezeigt, wenn Sie im ersten Schritt als Nutzungsmodus "Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen" ausgewählt haben.

Geben Sie in diesem Schritt die Rolle der virtuellen Maschine (Server oder Workstation) an, auf der Sie Kaspersky Endpoint Security installieren:

- Geben Sie `yes` ein, wenn Sie die virtuelle Maschine als Server verwenden.
- Geben Sie `no` ein, wenn Sie die virtuelle Maschine als Workstation verwenden.

Modus zum Schutz der VDI-Infrastruktur aktivieren

Dieser Schritt wird nur angezeigt, wenn Sie im ersten Schritt als Nutzungsmodus "Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen" ausgewählt haben.

In diesem Schritt können Sie den Modus zum Schutz der VDI-Infrastruktur aktivieren. Dieser Modus optimiert die Ausführung von Kaspersky Endpoint Security auf temporären virtuellen Maschinen. Wenn der Modus zum Schutz der VDI-Infrastruktur aktiviert ist, werden Updates, die einen Neustart der geschützten virtuellen Maschine erfordern, nicht installiert. Wenn Updates eingehen, die einen Neustart erfordern, sendet der auf einer virtuellen Maschine installierte Light Agent eine Nachricht an Kaspersky Security Center über die Notwendigkeit, die Vorlage der geschützten virtuellen Maschinen zu aktualisieren.

Geben Sie `yes` ein, wenn Sie den Modus zum Schutz der VDI-Infrastruktur aktivieren möchten. Dies wird empfohlen, wenn Kaspersky Endpoint Security auf einer Vorlage für virtuelle Maschinen installiert ist, aus der temporäre virtuelle Maschinen erstellt werden.

Geben Sie `no` ein, wenn Sie den Modus zum Schutz der VDI-Infrastruktur nicht aktivieren möchten. Dies wird empfohlen, wenn Kaspersky Endpoint Security auf einer dauerhaften virtuellen Maschine oder auf einer Vorlage für virtuelle Maschinen, aus der dauerhafte virtuelle Maschinen erstellt werden, installiert ist.

Gebietsschema auswählen

In diesem Schritt listet die App die Bezeichnungen der unterstützten Gebietsschemas in dem durch RFC 3066 bestimmten Format auf.

Geben Sie das Gebietsschema in dem Format an, in dem es in der Liste mit Bezeichnungen angeführt ist. Dieser Standard wird verwendet, um die an Kaspersky Security Center gesendeten App-Ereignisse sowie die Texte des Endbenutzer-Lizenzvertrags, der Datenschutzrichtlinie und der Erklärung zu Kaspersky Security Network zu lokalisieren.

Die Lokalisierung der grafischen Benutzeroberfläche und der Befehlszeile der App hängt von der Lokalisierung ab, die in der Umgebungsvariablen `LANG` angegeben ist. Wenn in der Umgebungsvariablen `LANG` eine Lokalisierung angegeben ist, die von der App Kaspersky Endpoint Security nicht unterstützt wird, werden die grafische Benutzeroberfläche und die Befehlszeile in der englischen Lokalisierung angezeigt.

Endbenutzer-Lizenzvertrag und Datenschutzrichtlinie lesen

In diesem Schritt sollten Sie sich mit dem Text des Endbenutzer-Lizenzvertrags, der zwischen Ihnen und Kaspersky geschlossen wird, sowie mit der Datenschutzrichtlinie, welche die Verarbeitung und Übermittlung von Daten beschreibt, vertraut machen.

Endbenutzer-Lizenzvertrag annehmen

In diesem Schritt müssen Sie die Bedingungen des Endbenutzer-Lizenzvertrags akzeptierten oder ablehnen.

Geben Sie nach Beendigung des Anzeigemodus einen der folgenden Werte ein:

- `yes` (oder `y`), wenn Sie mit den Bedingungen des Endbenutzer-Lizenzvertrags einverstanden sind.
- `no` (oder `n`), wenn Sie mit den Bedingungen des Endbenutzer-Lizenzvertrags nicht einverstanden sind.

Wenn Sie mit den Bedingungen des Endbenutzer-Lizenzvertrags nicht einverstanden sind, wird der Konfigurationsprozess der App Kaspersky Endpoint Security abgebrochen.

Annahme der Datenschutzrichtlinie

In diesem Schritt müssen Sie die Bedingungen der Datenschutzrichtlinie akzeptieren oder ablehnen.

Geben Sie nach Beendigung des Anzeigemodus einen der folgenden Werte ein:

- `yes` (oder `y`), wenn Sie mit den Bedingungen der Datenschutzrichtlinie einverstanden sind
- `no` (oder `n`), wenn Sie mit den Bedingungen der Datenschutzrichtlinie nicht einverstanden sind

Wenn Sie mit den Bedingungen der Datenschutzrichtlinie nicht einverstanden sind, wird der Konfigurationsprozess der App Kaspersky Endpoint Security abgebrochen.

Verwendung von Kaspersky Security Network

In diesem Schritt müssen Sie die Bedingungen zur Verwendung von Kaspersky Security Network entweder akzeptierten oder ablehnen. Die Datei "ksn_licence.<ID der Sprache>", die den Text der Erklärung zu Kaspersky Security Network enthält, befindet sich im Verzeichnis opt/kaspersky/kesl/doc/.

Geben Sie einen der folgenden Werte ein:

- `yes` (oder `y`), wenn Sie mit den Bedingungen der Erklärung zu Kaspersky Security Network einverstanden sind. Der erweiterte KSN-Modus wird aktiviert.
- `no` (oder `n`), wenn Sie mit den Bedingungen der Erklärung zu Kaspersky Security Network nicht einverstanden sind.

Wenn Sie die Verwendung von Kaspersky Security Network ablehnen, wird der Vorgang der Erstkonfiguration von Kaspersky Endpoint Security nicht unterbrochen. Sie können den Modus von Kaspersky Security Network jederzeit aktivieren, deaktivieren oder ändern.

Wenn Kaspersky Endpoint Security im Standard-Modus verwendet wird und Sie die Verwendung von Kaspersky Security Network aktiviert haben, wird automatisch der Cloud-Modus der App aktiviert. In diesem Modus verwendet Kaspersky Endpoint Security eine schlankere Version der Malware-Datenbanken. Im Light Agent-Modus zum Schutz virtueller Umgebungen wird die Verwendung der schlankeren Malware-Datenbanken nicht unterstützt.

Benutzer aus privilegierten Gruppen entfernen

Dieser Schritt wird nur angezeigt, wenn Benutzer in der Gruppe "kesladmin" und/oder in der Gruppe "keslaudit" gefunden werden.

Geben Sie in diesem Schritt an, ob die Benutzer aus den privilegierten Gruppen "kesladmin" und "keslaudit" entfernt werden sollen. Benutzer in den Gruppen "kesladmin" und "keslaudit" erhalten privilegierten Zugriff auf die Funktionen der App.

Geben Sie `yes` ein, um alle erkannten Benutzer aus der Gruppe "kesladmin" und/oder "keslaudit" zu entfernen. Benutzer, für welche die Gruppen "kesladmin" oder "keslaudit" die primären Gruppen darstellen, werden in die Gruppe "nogroup" verschoben. Wenn die Gruppe "nogroup" nicht vorhanden ist, wird die Installation unterbrochen und werden Sie aufgefordert, die Benutzer manuell aus den privilegierten Gruppen zu entfernen.

Geben Sie `no` ein, wenn Sie nicht möchten, dass die App die Benutzer aus den privilegierten Gruppen entfernt.

Einem Benutzer die Administratorrolle zuweisen

In diesem Schritt können Sie einem Benutzer die Rolle des Administrators (admin) zuweisen.

Geben Sie den Namen des Benutzers ein, dem Sie die Administratorrolle zuweisen möchten.

Sie können auch zu einem späteren Zeitpunkt einem Benutzer die Administratorrolle zuweisen.

Typ des Abfangmoduls für Dateioperationen festlegen

In diesem Schritt wird der Typ des Moduls zum Abfangen von Dateioperationen festgelegt. Für Betriebssysteme, von denen die fanotify-Technologie nicht unterstützt wird, muss die Kompilation des Kernelmoduls ausgeführt werden.

Werden die notwendigen Pakete im Laufe der Kompilierung des Kernelmoduls nicht gefunden, so schlägt Kaspersky Endpoint Security vor, diese zu installieren. Wenn das Herunterladen der Pakete fehlschlägt, wird eine Fehlermeldung ausgegeben.

Wenn alle notwendigen Pakete installiert wurden, wird das Kernel-Modul beim Start der Aufgabe "Schutz vor bedrohlichen Dateien" automatisch kompiliert.

Sie können die Kompilation des Kernel-Moduls später, nach Abschluss der Erstkonfiguration der App Kaspersky Endpoint Security ausführen.

Automatische Konfiguration von SELinux aktivieren

Dieser Schritt erscheint nur, wenn das SELinux-Modul in Ihrem Betriebssystem installiert ist.

In diesem Schritt können Sie die automatische Konfiguration des SELinux-Systems für Kaspersky Endpoint Security aktivieren.

Geben Sie `yes` ein, um die automatische Konfiguration des SELinux-Systems zu aktivieren. Wenn die automatische Konfiguration des SELinux-Systems fehlschlägt, gibt die App eine Fehlermeldung aus und fordert den Benutzer aus, das SELinux-System manuell zu konfigurieren.

Geben Sie `no` ein, wenn Sie nicht möchten, dass die App das SELinux-System automatisch konfiguriert.

Standardmäßig wird von der App der Wert `yes` vorgeschlagen.

Falls erforderlich, können Sie später das SELinux-System manuell für die Arbeit mit der App konfigurieren, nachdem die Erstkonfiguration der App Kaspersky Endpoint Security abgeschlossen ist.

Update-Quelle konfigurieren

Dieser Schritt wird nur angezeigt, wenn Sie im ersten Schritt als Nutzungsmodus für Kaspersky Endpoint Security den Standard-Modus ausgewählt haben. Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, bezieht Kaspersky Endpoint Security die Updates für die Datenbanken und App-Module von Light Agent über den Schutzserver.

In diesem Schritt müssen Sie die Quelle für die Updates der Datenbanken und Module der App angeben.

Geben Sie einen der folgenden Werte ein:

- `KLServers` – Die App erhält die Updates von einem der Kaspersky-Update-Server.
- `SCServer` – Die App lädt die Updates von einem in Ihrer Organisation installierten Administrationsserver für Kaspersky Security Center auf das geschützte Gerät herunter. Sie können diese Updatequelle auswählen, wenn Sie die App Kaspersky Security Center für die zentrale Verwaltung des Schutzes der Geräte in Ihren Unternehmen benutzen.

- < Webadresse > – Die App lädt Updates aus einer benutzerdefinierten Quelle herunter. Sie können die Adresse der benutzerdefinierten Update-Quelle im lokalen Netzwerk oder im Internet festlegen.
- < Pfad > – Die App ruft die Updates aus dem angegebenen Verzeichnis ab.

Allgemeine Proxy-Server-Einstellungen anpassen

Dieser Schritt wird nur angezeigt, wenn Sie im ersten Schritt als Nutzungsmodus für Kaspersky Endpoint Security den Standard-Modus ausgewählt haben.

In diesem Schritt müssen Sie die Einstellungen des Proxy-Servers angeben, den Sie für den Internetzugang verwenden. Der Download der App-Datenbanken von den Update-Servern erfordert eine Internetverbindung.

Führen Sie eine der folgenden Aktionen aus, um die Einstellungen des Proxy-Servers anzupassen:

- Wenn Sie für die Internetverbindung einen Proxy-Server verwenden, geben Sie die Adresse des Proxy-Servers in einem der folgenden Formate an:
  - < IP-Adresse des Proxy-Servers >:< Portnummer >, wenn für die Verbindung zum Proxy-Server keine Authentifizierung erforderlich ist
  - < Benutzername >:< Kennwort >@< IP-Adresse des Proxy-Servers >:< Portnummer >, wenn für die Verbindung zum Proxy-Server eine Authentifizierung erforderlich ist

    Für die Verbindung über einen Proxy-Server mittels HTTP-Protokoll wird empfohlen, ein separates Konto zu verwenden, das nicht zur Authentifizierung in anderen Systemen verwendet wird. Der HTTP-Proxy-Server verwendet eine unsichere Verbindung und dessen Konto kann kompromittiert werden.
- Wenn Sie für die Internetverbindung keinen Proxy-Server verwenden, geben Sie die Antwort no ein.

Standardmäßig wird von der App der Wert no vorgeschlagen.

Sie können die Einstellungen für den Proxy-Server auch später konfigurieren, ohne das Skript für die Erstkonfiguration zu verwenden.

Update der App-Datenbanken starten

Dieser Schritt wird nur angezeigt, wenn Sie im ersten Schritt als Nutzungsmodus für Kaspersky Endpoint Security den Standard-Modus ausgewählt haben. Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, bezieht Kaspersky Endpoint Security die Updates für die Datenbanken und App-Module von Light Agent über den Schutzserver.

In diesem Schritt können Sie die Aufgabe zum Update der App-Datenbanken auf dem Client-Gerät starten. Die App-Datenbanken enthalten Beschreibungen der Signaturen von Bedrohungen und der Methoden zu ihrer Bekämpfung. Die App verwendet diese Einträge bei der Suche und der Neutralisierung von Bedrohungen. Die Virenanalysten von Kaspersky fügen regelmäßig Einträge über Bedrohungen hinzu.

Wenn Sie auf das Starten des Updates der App-Datenbanken verzichten möchten, geben Sie no ein.

Wenn Sie die Aufgabe zum Update der Datenbanken auf dem Gerät starten möchten, geben Sie `yes` ein.

Standardmäßig wird von der App der Wert `yes` vorgeschlagen.

Wenn `yes` ausgewählt ist, wird die App nach dem Update der Datenbanken automatisch neu gestartet.

Kaspersky Endpoint Security kann den vollständigen Schutz des Geräts erst nach dem Update der App-Datenbanken sicherstellen.

Sie können die Update-Aufgabe später starten, ohne das Skript zur Erstkonfiguration zu verwenden.

Automatische Updates für die App-Datenbanken aktivieren

Dieser Schritt wird nur angezeigt, wenn Sie im ersten Schritt als Nutzungsmodus für Kaspersky Endpoint Security den Standard-Modus ausgewählt haben. Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, bezieht Kaspersky Endpoint Security die Updates für die Datenbanken und App-Module von Light Agent über den Schutzserver.

In diesem Schritt können Sie das automatische App-Datenbanken-Update aktivieren.

Geben Sie `yes` ein, um das automatische App-Datenbanken-Update zu aktivieren. Standardmäßig prüft die App alle 60 Minuten, ob Datenbanken-Updates vorhanden sind. Wenn Updates verfügbar sind, lädt die App die aktualisierten Datenbanken herunter.

Geben Sie `no` ein, wenn Sie nicht möchten, dass die App die Datenbanken automatisch aktualisiert.

Sie können die automatischen Datenbanken-Updates später aktivieren, ohne das Skript zur Erstkonfiguration zu verwenden, indem Sie einen Zeitplan für die Update-Aufgabe einrichten.

App aktivieren

Dieser Schritt wird nur angezeigt, wenn Sie im ersten Schritt als Nutzungsmodus für Kaspersky Endpoint Security den Standard-Modus ausgewählt haben. Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, erhält Kaspersky Endpoint Security die Lizenzinformationen vom Schutzserver. Ein separates Aktivieren von Kaspersky Endpoint Security ist nicht erforderlich.

In diesem Schritt können Sie die App mithilfe eines Aktivierungscodes oder einer Schlüsseldatei aktivieren.

Um die App mithilfe eines Aktivierungscodes zu aktivieren, müssen Sie den Aktivierungscode eingeben.

Um die App mithilfe einer Schlüsseldatei zu aktivieren, müssen Sie den vollständigen Pfad der Schlüsseldatei angeben.

Wenn Sie keinen Aktivierungscode bzw. keine Schlüsseldatei angegeben haben, wird die App mithilfe eines Testschlüssels für einen Monat aktiviert.

Sie können die App später aktivieren, ohne das Skript zur Erstkonfiguration zu verwenden.

Ersteinrichtung der App im automatischen Modus

Sie können die Erstkonfiguration der App im automatischen Modus ausführen.

Um die Erstkonfiguration der App im automatischen Modus zu starten, führen Sie den folgenden Befehl aus:

```
# /opt/kaspersky/kesl/bin/kesl-setup.pl --autoinstall=< Konfigurationsdatei für die Erstkonfiguration >
```

wobei < `Konfigurationsdatei für die Erstkonfiguration` > für den Pfad der Konfigurationsdatei steht, welche die Einstellungen für die Ersteinrichtung enthält. Sie können diese Datei erstellen oder ihre Struktur aus der Konfigurationsdatei "autoinstall.ini" kopieren, die zur Remote-Installation der App mithilfe von Kaspersky Security Center verwendet wird.

Wenn das automatische Skript zur Erstkonfiguration abgeschlossen ist und die Befehlszeile freigibt, ist der Prozess der Erstkonfiguration der App beendet.

Um den Rückgabe-Code zu prüfen, führen Sie den folgenden Befehl aus:

```
echo $?
```

Wenn der Code 0 zurückgegeben wird, ist die Erstkonfiguration der App erfolgreich abgeschlossen.

Nach Abschluss des Skripts müssen Sie für ein fehlerfreies Update der App-Module die App möglicherweise neu starten. Sie können den Update-Status der App mit dem Befehl `kesl-control --app-info` überprüfen.

Einstellungen der Konfigurationsdatei für die Erstkonfiguration

In der Konfigurationsdatei für die Erstkonfiguration können Sie die in der folgenden Tabelle aufgeführten Parameter festlegen. Der Umfang der anwendbaren Einstellungen, hängt dabei vom Nutzungsmodus der App ab.

Einstellungen der Konfigurationsdatei für die Erstkonfiguration

Einstellung	Beschreibung	Werte
KSVLA_MODE	Nutzungsmodus von Kaspersky Endpoint Security.	`yes` – Kaspersky Endpoint Security wird im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet (im Rahmen von Kaspersky Security for Virtualization Light Agent). `no` – Kaspersky Endpoint Security wird im Standard-Modus verwendet.
SERVER_MODE	Rolle der geschützten virtuellen Maschine (Server oder Workstation). Die Einstellung wird nur angewendet, wenn die App im Light Agent-Modus verwendet wird.	`yes` – Die geschützte virtuelle Maschine wird als Server verwendet. `no` – Die geschützte virtuelle Maschine wird als Workstation verwendet.

VDI_MODE	Aktivieren des Modus zum Schutz der VDI-Infrastruktur, um die Leistung der App auf temporären virtuellen Maschinen zu optimieren. Die Einstellung wird nur angewendet, wenn die App im Light Agent-Modus verwendet wird.	yes – Modus zum Schutz der VDI-Infrastruktur aktivieren. Dies wird empfohlen, wenn Kaspersky Endpoint Security auf einer Vorlage für virtuelle Maschinen installiert ist, aus der temporäre virtuelle Maschinen erstellt werden. no – Modus zum Schutz der VDI-Infrastruktur nicht aktivieren.
EULA_AGREED	Erforderliche Einstellung. Annahme der Bedingungen des Endbenutzer-Lizenzvertrags.	yes – Sie müssen die Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren, damit Sie mit dem Installationsprozess der App fortfahren können. no – Bedingungen des Endbenutzer-Lizenzvertrags nicht akzeptieren. Die Installation der App wird abgebrochen.
PRIVACY_POLICY_AGREED	Erforderliche Einstellung. Zustimmung zu den Bedingungen der Datenschutzrichtlinie.	yes – Sie müssen die Bedingungen der Datenschutzrichtlinie akzeptieren, um mit der Installation der App fortfahren zu können. no – Bedingungen der Datenschutzrichtlinie nicht akzeptieren. Die Installation der App wird abgebrochen.
USE_KSN	Erforderliche Einstellung. Verwendung von Kaspersky Security Network aktivieren. Um die Nutzung von KSN zu aktivieren, müssen Sie die Bedingungen der Erklärung zu Kaspersky Security Network akzeptieren.	yes – Bedingungen der Erklärung zu Kaspersky Security Network-akzeptieren und die Verwendung von KSN aktivieren. no – Bedingungen der Erklärung zu Kaspersky Security Network nicht akzeptieren. Wenn Kaspersky Endpoint Security im Standard-Modus verwendet wird und Sie die Verwendung von KSN aktiviert haben, wird automatisch der Cloud-Modus der App aktiviert. In diesem Modus verwendet Kaspersky Endpoint Security eine schlankere Version der Malware-Datenbanken.
GROUP_CLEAN	Erforderliche Einstellung. Entfernen von Benutzern aus den privilegierten Gruppen "kesladmin" und "keslaudit".	yes – Die Benutzer werden aus den privilegierten Gruppen entfernt. Wenn der Wert yes angegeben wurden und die Gruppe "nogroup" nicht vorhanden ist, wird die Installation unterbrochen und werden Sie aufgefordert, die Benutzer manuell aus den privilegierten Gruppen zu entfernen. no – Die Benutzer werden nicht aus den privilegierten Gruppen entfernen.

LOCALE	Optionale Einstellung. Gebietsschema, das für die Lokalisierung von Ereignissen in der App verwendet wird, die an Kaspersky Security Center gesendet werden.	Das Gebietsschema wird mittels RFC 3066-Format angegeben. Wird die Einstellung `LOCALE` nicht angegeben, so wird das Gebietsschema des Betriebssystems verwendet. Wenn die App keine Sprachversion des Betriebssystems bestimmen konnte oder das Betriebssystem diese Lokalisierung nicht unterstützt, wird standardmäßig `en_US.utf8` installiert. Die Lokalisierung der grafischen Benutzeroberfläche und der Befehlszeile der App hängt von der Lokalisierung ab, die in der Umgebungsvariablen `LANG` angegeben ist. Wenn in der Umgebungsvariablen `LANG` eine Lokalisierung angegeben ist, die von der App Kaspersky Endpoint Security nicht unterstützt wird, werden die grafische Benutzeroberfläche und die Befehlszeile in der englischen Lokalisierung angezeigt.
INSTALL_LICENSE	Aktivierungscode oder Schlüsseldatei Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.	
UPDATER_SOURCE	Update-Quelle Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.	`SCServer` – Administrationsserver von Kaspersky Security Center als Update-Quelle verwenden `KLServers` – die Kaspersky-Update-Server als Update-Quelle verwenden Adresse der Update-Quelle
PROXY_SERVER	Adresse des Proxy-Servers, der für die Internetverbindung verwendet wird Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.	Adresse des Proxy-Servers
UPDATE_EXECUTE	Aufgabe zum Update der App-Datenbanken während des Konfigurationsvorgangs starten	`yes` – Update-Aufgabe starten `no` – Update-Aufgabe nicht starten

	Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.	
KERNEL_SRCS_INSTALL	Automatischer Start der Kompilierung des Kernelmoduls	`yes` – Kernelmodul kompilieren `no` – Kernel-Modul nicht kompilieren
ADMIN_USER	Benutzer, dem die Administratorrolle (admin) zugewiesen ist.	
CONFIGURE_SELINUX	Automatische Konfiguration von SELinux für die Arbeit mit der App Kaspersky Endpoint Security.	`yes` – Automatische Konfiguration von SELinux für die Arbeit mit Kaspersky Endpoint Security ausführen. `no` – Automatische Konfiguration von SELinux für die Arbeit mit Kaspersky Endpoint Security nicht ausführen.
DISABLE_PROTECTION	Deaktivieren der Schutzkomponenten und der Aufgaben Untersuchungsaufgaben der App, nachdem sie installiert wurde. Eine Installation mit deaktivierten Schutzkomponenten kann hilfreich sein, um beispielsweise ein Problem mit der App zu reproduzieren und eine Protokolldatei zu erstellen. Wenn Sie nach der App-Installation mit dem Parameter `DISABLE_PROTECTION=yes` die erforderlichen Komponenten und Aufgaben aktivieren, werden die aktivierten Komponenten und Aufgaben nach einem Neustart der App ausgeführt.	`yes` – Schutzkomponenten und Untersuchungsaufgaben beim ersten Start der App nach deren Installation deaktivieren. `no` – Schutzkomponenten und Untersuchungsaufgaben beim ersten Start der App nach deren Installation nicht deaktivieren.
DISABLE_FILEAV_ACTIONS	Deaktivieren der Desinfektions- und Dateilöschfunktionen für Komponenten der App, nachdem sie installiert wurde.	`yes` – Desinfektions- und Dateilöschfunktionen beim Starten der App nach der Installation deaktivieren. `no` (Standardwert) – Desinfektions- und Dateilöschfunktionen beim Starten der App nach der Installation nicht deaktivieren.

	Wenn die Desinfektions- und Dateilöschfunktionen deaktiviert sind und eine Bedrohung erkannt wird, versucht die App nicht, Dateien zu desinfizieren oder zu löschen, in denen eine Bedrohung erkannt wurde, sondern informiert den Benutzer lediglich darüber, dass eine Bedrohung erkannt wurde. Nach der Installation der App können Sie die Funktionen zum Desinfizieren und Löschen von Dateien mithilfe des Parameters `DisableFileAvActions` in der Konfigurationsdatei kesl.ini aktivieren.	

Wenn Sie die Einstellungen in der Konfigurationsdatei für die Erstkonfiguration ändern möchten, geben Sie die Werte für die Einstellungen im Format <Name der Einstellung>=<Einstellungswert> ein (die App verarbeitet keine Leerzeichen zwischen dem Namen der Einstellung und ihrem Wert).

Konfiguration der Berechtigungen im SELinux-System

Manuelle Konfiguration von SELinux für die Arbeit mit der App

Wenn bei der Ersteinrichtung der App Kaspersky Endpoint Security das SELinux-System nicht automatisch konfiguriert werden konnte oder Sie die automatische Konfiguration abgelehnt haben, können Sie das SELinux-System manuell für die Arbeit mit der App Kaspersky Endpoint Security konfigurieren.

So konfigurieren Sie SELinux für die Arbeit mit der App manuell:

1. Schalten Sie SELinux in den Erlaubnismodus:
   - Wenn SELinux aktiviert wurde, führen Sie den folgenden Befehl aus:

     ```
     # setenforce Permissive
     ```

   - Falls SELinux deaktiviert wurde, geben Sie in der Konfigurationsdatei /etc/selinux/config den Parameterwert `SELINUX=permissive` an und starten Sie das Betriebssystem neu.
2. Stellen Sie sicher, dass das Tool semanage im System installiert ist. Wenn das Tool nicht installiert ist, installieren Sie je nach Typ des Paketmanagers das Paket policycoreutils-python oder policycoreutils-python-utils.
3. Wenn Sie eine benutzerdefinierte SELinux-Richtlinie verwenden, die sich von der Standardrichtlinie targeted policy unterscheidet, kennzeichnen Sie die folgenden ausführbaren Quelldateien der App Kaspersky Endpoint Security gemäß der verwendeten SELinux-Richtlinie:
   - /var/opt/kaspersky/kesl/12.1.0.<Buildnummer>_<Installationszeitstempel>/opt/kaspersky/kesl/libexec/kesl

- /var/opt/kaspersky/kesl/12.1.0<Buildnummer>_<Installationszeitstempel>/opt/kaspersky/kesl/bin/kesl-control
- /var/opt/kaspersky/kesl/12.1.0<Buildnummer>_<Installationszeitstempel>/opt/kaspersky/kesl/libexec/kesl-gui
- /var/opt/kaspersky/kesl/12.1.0<Build-Nummer>_<Installationszeitstempel>/opt/kaspersky/kesl/shared/kesl

4. Führen Sie den folgenden Aufgaben aus:

   - Aufgabe zum Schutz vor bedrohlichen Dateien:

     ```
     kesl-control --start-task 1
     ```

   - Aufgabe zur Untersuchung wichtiger Bereiche:

     ```
     kesl-control --start-task 4 -W
     ```

   Es wird empfohlen, alle geplanten Aufgaben während der Verwendung der App Kaspersky Endpoint Security auszuführen.

5. Starten Sie die grafische Benutzeroberfläche, wenn Sie diese benutzen wollen.

6. Stellen Sie sicher, dass in der Datei "audit.log" keine Fehler enthalten sind:

   ```
   grep kesl /var/log/audit/audit.log
   ```

7. Sollten in der Datei audit.log Fehler enthalten sein, erstellen Sie ein neues Regelmodul und führen Sie es auf der Grundlage der blockierenden Einträge aus, um die Fehler zu beheben. Führen Sie anschließend alle Aufgaben erneut aus, die Sie für die Ausführung in der App Kaspersky Endpoint Security geplant haben.

   Wenn neue Audit-Meldungen erscheinen, die sich auf Kaspersky Endpoint Security beziehen, muss die Datei des Regelmoduls aktualisiert werden.

8. Schalten Sie SELinux in den Sperrmodus:

   ```
   # setenforce Enforcing
   ```

Wenn Sie eine benutzerdefinierte SELinux-Richtlinie verwenden, müssen Sie nach der Installation von App-Updates den ursprünglichen ausführbaren Dateien der App Kaspersky Endpoint Security manuell eine Kennzeichnung zuweisen (befolgen Sie die Schritte 1, 3–8).

Weitere Informationen finden Sie in der Dokumentation des jeweiligen Betriebssystems.

Konfiguration von SELinux für die Ausführung der Aufgaben "Prozess starten".

Wenn auf Ihrem Betriebssystem SELinux im Modus `Enforcing` installiert ist, müssen Sie zum Ausführen der Aufgabe Prozess starten zusätzlich das SELinux-System konfigurieren.

So konfigurieren Sie SELinux für die Ausführung der Aufgabe "Prozess starten":

1. Schalten Sie SELinux in den Erlaubnismodus:

- Wenn SELinux aktiviert wurde, führen Sie den folgenden Befehl aus:

  ```
  # setenforce Permissive
  ```

- Falls SELinux deaktiviert wurde, geben Sie in der Konfigurationsdatei /etc/selinux/config den Parameterwert `SELINUX=permissive` an und starten Sie das Betriebssystem neu.

2. Stellen Sie sicher, dass das Tool semanage im System installiert ist. Wenn das Tool nicht installiert ist, installieren Sie je nach Typ des Paketmanagers das Paket policycoreutils-python oder policycoreutils-python-utils.

3. Führen Sie die Aufgabe "Prozess starten" aus.

4. Stellen Sie sicher, dass in der Datei "audit.log" keine Fehler enthalten sind:

   ```
   grep kesl /var/log/audit/audit.log
   ```

5. Wenn die Datei audit.log Fehler enthält, erstellen und laden Sie eine neues Regel-Modul basierend auf blockierenden Einträgen, um die Fehler zu beheben. Führen Sie die Aufgabe "Prozess starten" anschließend erneut aus.

6. Schalten Sie SELinux in den Sperrmodus:

   ```
   # setenforce Enforcing
   ```

App im Betriebssystem Astra Linux im Modus für abgeschlossene Softwareumgebungen starten

In diesem Abschnitt werden die Aktionen beschrieben, die Sie ausführen müssen, um die App unter Astra Linux Special Edition zu starten.

Für Astra Linux Special Edition (operational Update 1.7) und Astra Linux Special Edition (operational Update 1.6)

So starten Sie die App unter dem Betriebssystemen Astra Linux Special Edition (reguläres Update 1.7) oder Astra Linux Special Edition (reguläres Update 1.6):

1. Geben Sie in der Datei /etc/digsig/digsig_initramfs.conf die folgende Einstellung an:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Installieren Sie das Kompatibilitätspaket:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Erstellen Sie ein Verzeichnis für den App-Schlüssel:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Finden Sie den App-Schlüssel (/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg) im Verzeichnis, das Sie im vorherigen Schritt erstellt haben:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. Aktualisieren Sie das initramfs-Image:

   ```
   update-initramfs -u -k all
   ```

Für Astra Linux Special Edition (operational Update 1.5)

So starten Sie die App unter dem Betriebssystem Astra Linux Special Edition (reguläres Update 1.5):

1. Geben Sie in der Datei /etc/digsig/digsig_initramfs.conf die folgende Einstellung an:

   ```
   DIGSIG_LOAD_KEYS=1
   DIGSIG_ENFORCE=1
   ```

2. Erstellen Sie ein Verzeichnis für den App-Schlüssel:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

3. Finden Sie den App-Schlüssel (/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg) im Verzeichnis, das Sie im vorherigen Schritt erstellt haben:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

4. Aktualisieren Sie das initramfs-Image:

   ```
   sudo update-initramfs -u -k all
   ```

Die Verwendung der grafischen Benutzeroberfläche der App wird für Sitzungen mit Mandatory Access Control unterstützt.

Update einer Vorgängerversion der App durchführen

Ein Upgrade auf Kaspersky Endpoint Security 12.1 für Linux ist nur für die Version Kaspersky Endpoint Security 12.0 für Linux möglich.

Es ist nicht möglich, Kaspersky Endpoint Security von früheren Versionen auf Version 12.1 zu aktualisieren. Wenn Sie eine frühere Version von Kaspersky Endpoint Security installiert haben, müssen Sie diese zunächst deinstallieren und anschließend Kaspersky Endpoint Security 12.1 für Linux installieren.

Bevor Sie mit der Aktualisierung von Kaspersky Endpoint Security beginnen, müssen Sie die Installation vorbereiten.

Die Aktualisierung der App besteht aus den folgenden Schritten:

1. **Aktualisieren des Kaspersky Security Center Administrationsagenten**

   Wenn Sie Kaspersky Endpoint Security mithilfe von Kaspersky Security Center verwalten, müssen Sie auf den geschützten Geräten den Administrationsagenten aktualisieren. Das Update wird mittels Installation einer neuen Version des Administrationsagenten durchgeführt.

   Wenn der Administrationsagent nicht aktualisiert wurde, kann die App nicht über Kaspersky Security Center verwaltet werden.

   > Auf einem Gerät, auf dem das Betriebssystem Astra Linux Special Edition ausgeführt wird, sollte der Administrationsagenten per Fernzugriff über Kaspersky Security Center aktualisiert werden. Bei einer Aktualisierung über die Befehlszeile in der Verwaltungskonsole von Kaspersky Security Center wird ein neues Objekt von dem verwalteten Gerät erstellt, während das alte nicht mehr verfügbar ist.

   Während des Updates des Administrationsagenten funktioniert die App weiterhin ordnungsgemäß.

2. **Aktualisieren des Verwaltungs-Plug-ins für Kaspersky Endpoint Security**

   Wenn Sie Kaspersky Endpoint Security mithilfe von Kaspersky Security Center verwalten, müssen Sie je nach verwendeter Verwaltungskonsole von das Web-Plug-in von Kaspersky Endpoint Security oder das MMC-basierte Plug-in zum Verwalten aktualisieren.

3. **Aktualisieren der App und der grafischen Benutzeroberfläche auf geschützten Geräten**

   Sie müssen die auf den geschützten Geräten installierte App aktualisieren. Die aktualisierte App übernimmt den Nutzungsmodus, der bei der Installation ausgewählt wurde. Wenn Sie die App in einem anderen Modus verwenden möchten, müssen Sie die App zunächst deinstallieren und anschließend die Installationsprozedur und die Konfiguration zur Ersteinrichtung der App durchführen.

   Wenn Kaspersky Endpoint Security im Standard-Modus verwendet wird und Sie die grafische Benutzeroberfläche der App verwenden, müssen Sie auch die grafische Benutzeroberfläche aktualisieren.

   Sie können die App und die grafische Benutzeroberfläche der App auf folgende Weise aktualisieren:

   - Per Fernzugriff über Kaspersky Security Center.
   - Lokal über die Befehlszeile.

> Wenn während des App-Upgrades ein Fehler auftritt, wird ein Rollback ausgeführt und die Vorgängerversion der App gestartet. In diesem Fall wird eine Fehlermeldung angezeigt, aber der Paketmanager zeigt die neue Version (rpm/dpkg) an.

Unabhängig davon, ob die App Kaspersky Endpoint Security vor dem Start des Update-Vorgangs gestartet wurde, wird nach dem erfolgreichen Abschluss des Updates die neue App-Version gestartet.

Wenn Sie die Version der App aktualisieren, werden die Dump-Dateien vorheriger Versionen gelöscht.

Wenn Sie Kaspersky Endpoint Security im Standard-Modus verwenden, wird es empfohlen, nach dem App-Update die Aufgabe zum Datenbank-Update auszuführen.

Informationen zum Aktualisieren der Verwaltungs-Plug-ins für Kaspersky Endpoint Security

Die Aktualisierung des Verwaltungs-Plug-ins für Kaspersky Endpoint Security erfolgt durch die Installation einer neuen Version des Verwaltungs-Plug-ins. Abhängig von der Verwaltungskonsole von Kaspersky Security Center, die Sie verwenden, müssen Sie Folgendes installieren:

- Web-Plug-in für die Verwaltung von Kaspersky Endpoint Security;
- MMC-Plug-in für die Verwaltung von Kaspersky Endpoint Security.

Richtlinien und Aufgaben, die für Kaspersky Endpoint Security 12.0 für Linux konfiguriert wurden, sind nicht mit der aktualisierten Version der App kompatibel. Wenn Sie zum Verwalten der App die Verwaltungskonsole von Kaspersky Security Center verwenden, können Sie nach der Aktualisierung des MMC-Plug-ins für die Verwaltung die Richtlinien und Aufgaben mithilfe des Assistenten für die Massenkonvertierung von Richtlinien und Aufgaben in Kaspersky Security Center konvertieren (weitere Informationen dazu finden Sie in der Hilfe von Kaspersky Security Center).

In den konvertierten Richtlinien und Aufgaben werden für die meisten Parameter die Werte verwendet, die bereits für die vorherige Version der App konfiguriert wurden. Einige Parameter verfügen über spezielle Werte. Parameter, die in den Richtlinien und Aufgaben der vorherigen Version nicht enthalten waren, übernehmen in den konvertierten Richtlinien und Aufgaben die vorgesehenen Standardwerte.

Das Verfahren zum Konvertieren von Richtlinien und Aufgaben ist in der Kaspersky Security Center Web Console nicht verfügbar. Wenn Sie zur Verwaltung der App die Web Console verwenden, müssen Sie in Kaspersky Security Center neue Richtlinien und Aufgaben für die App erstellen. Einige Parameterwerte von Richtlinien und Aufgaben können Sie aus der vorherigen Version der Richtlinien oder Aufgaben auf die neue übertragen, indem Sie Einstellungen exportieren und importieren.

Ältere Versionen der Verwaltungs-Plug-ins funktionieren auch nach der Installation einer neuen Version der Verwaltungs-Plug-ins für Kaspersky Endpoint Security weiterhin. Mit ihrer Hilfe können Sie die vorherige Version von Kaspersky Endpoint Security verwalten.

Wenn Sie die App auf allen Client-Geräten aktualisiert haben, können Sie die Verwaltungs-Plug-ins für Kaspersky Endpoint Security der vorherigen Version entfernen.

Update der App mithilfe von Kaspersky Security Center durchführen

Die Aktualisierung der App und der grafischen Benutzeroberfläche erfolgt durch die Remote-Installation einer neuen Version der Pakete für die App und die grafische Benutzeroberfläche auf dem geschützten Gerät.

Die grafische Benutzeroberfläche wird nicht unterstützt, wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden.

Für die Remote-Installation wird ein Installationspaket für Kaspersky Endpoint Security verwendet. Sie können ein Installationspaket über die Kaspersky Security Center Web Console oder über die Verwaltungskonsole erstellen.

Die Kaspersky Security Center Web Console unterstützt die folgenden Hauptszenarien der Bereitstellung:

- App mithilfe des Assistenten für die Bereitstellung des Schutzes installieren.
- App über die Aufgabe zur Remote-Installation der App installieren.

Die Kaspersky Security Center Verwaltungskonsole unterstützt die folgenden hauptsächlichen Bereitstellungsmethoden:

- App über den Assistenten für Remote-Installationen installieren.
- App über die Aufgabe zur Remote-Installation der App installieren.

Eine Beschreibung der Bereitstellungsmethoden finden Sie in der Hilfe zu Kaspersky Security Center.

Update der App über die Befehlszeile durchführen

Die Aktualisierung der App über die Befehlszeile erfolgt durch die Installation einer neuen Version der App auf dem Gerät aus einem RPM- oder DEB-Paket entsprechend dem Typ des Paketmanagers.

Wenn Sie eine grafische Benutzeroberfläche verwenden, müssen Sie zum Aktualisieren zunächst die vorherige Version des Pakets für die grafische Benutzeroberfläche mit dem Befehl `rpm -e --nodeps kesl-gui` deinstallieren und dann das Paket mit den Dateien für die Version 12.1 der grafischen Benutzeroberfläche installieren.

> Die grafische Benutzeroberfläche wird nicht unterstützt, wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden.

Wenn sich in der neuen Version der App die Bedingungen des Endbenutzer-Lizenzvertrags und/oder der Datenschutzrichtlinie geändert haben, müssen Sie während des Updates die neuen Bedingungen akzeptieren. Bitte lesen Sie die neue Version des Endbenutzer-Lizenzvertrags und/oder der Datenschutzrichtlinie:

- Die neue Version des Endbenutzer-Lizenzvertrags findet sich im Verzeichnis (~/.kesl/<App-Version>/license.<ID der Sprache>).
- Die neue Version der Datenschutzrichtlinie findet sich im Verzeichnis (~/.kesl/<App-Version>/license.<ID der Sprache>).

Wenn Sie den Bedingungen des Endbenutzer-Lizenzvertrags und/oder der Datenschutzrichtlinie nicht zustimmen, erfolgt kein Update der App.

Wenn sich die Bedingungen der Erklärung zu Kaspersky Security Network in der neuen Version der App geändert haben, müssen Sie die neuen Bedingungen für Verwendung von Kaspersky Security Network akzeptieren oder ablehnen. Lesen Sie die neue Version des Dokuments im Verzeichnis (~/.kesl/<App-Version>/ksn_license.<ID der Sprache>). Wenn Sie die Verwendung von Kaspersky Security Network ablehnen, wird der Update-Vorgang von Kaspersky Endpoint Security nicht unterbrochen. Sie können den Modus von Kaspersky Security Network später aktivieren, deaktivieren oder ändern.

Wenn Sie in der vorherigen Version der App KSN verwendet und die Bedingungen der Erklärung zu Kaspersky Security Network akzeptiert haben, müssen Sie die Bedingungen der Erklärung zu Kaspersky Security Network bei Aktualisierung der App-Version erneut akzeptieren. Andernfalls wird die Nutzung von KSN deaktiviert.

Um die Bedingungen der neuen Vereinbarungen während des Updates zu akzeptieren, verwenden Sie die Umgebungsvariablen `KESL_EULA_AGREED=yes`, `KESL_PRIVACY_POLICY_AGREED=yes` und `KESL_USE_KSN=yes/no`.

So aktualisieren Sie die App:

1. Installieren Sie das App-Paket je nach verwendetem Paketmanager mit dem folgenden Befehlen. Wenn Sie die grafische Benutzeroberfläche für eine frühere Version der App installiert haben, müssen Sie auch das Paket installieren, das die Dateien der Benutzeroberfläche der App enthält.

   - Für ein Paket im RPM-Format:

     ```
     # [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] rpm -U --replacefiles --replacepkgs kesl-12.1.0-<Bild-Nummer>.<arch>.rpm [kesl-gui-12.1.0-<Bild-Nummer>.<arch>.rpm]
     ```

     wobei `<arch>` der Architektur entspricht:

     - i386 – für 32-Bit-Betriebssysteme
     - x86_64 – für 64-Bit-Betriebssysteme
     - aarch64 – für 64-Bit-Betriebssysteme für Arm

     Wenn Sie auf einem Betriebssystem mit rpm das App-Paket zusammen mit dem Paket für die grafische Benutzeroberfläche installiert haben, wird es nicht empfohlen, nur eines der Pakete zu aktualisieren.

   - Für ein Paket im DEB-Format:

     ```
     # [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] apt-get install ./kesl_12.1.0-<Bild-Nummer>_<arch>.deb [./kesl-gui_12.1.0-<Bild-Nummer>_<arch>.deb]
     ```

     wobei `<arch>` der Architektur entspricht:

     - i386 – für 32-Bit-Betriebssysteme
     - amd64 – für 64-Bit-Betriebssysteme
     - arm64 – für 64-Bit-Betriebssysteme für Arm

     Wenn Sie auf einem Betriebssystem mit dpkg das App-Paket zusammen mit dem Paket für die grafische Benutzeroberfläche installiert haben, ist es nicht möglich, nur eines der Pakete zu aktualisieren.

2. Kaspersky Endpoint Security wird automatisch neu gestartet.

3. Bei einigen Betriebssystemen müssen Sie möglicherweise das Betriebssystem neu starten, wenn die App eine entsprechende Meldung anzeigt.

Wenn Sie die App über die Befehlszeile verwalten, verwenden die meisten Parameter nach dem Update die Werte, die bereits in der vorherigen Version der App konfiguriert wurden. Einige Parameter verfügen über spezielle Werte. Parameter, die in der vorherigen Version der App nicht vorhanden waren, übernehmen in der neuen Version der App die vorgesehenen Standardwerte.

Änderungen an den App-Einstellungen, die Sie nach Abschluss der Aktualisierung und vor dem Neustart der App vornehmen, werden nicht gespeichert.

Besonderheiten beim Festlegen von Parameterwerten während eines App-Updates

Wenn Sie zur Verwaltung der App die Verwaltungskonsole von Kaspersky Security Center verwenden und nach dem Update der App die Werte der Richtlinien- und Aufgabeneinstellungen verwenden möchten, die in Kaspersky Security Center bereits für die vorherige Version der App konfiguriert wurden, müssen Sie die Konvertierung der Richtlinien und Aufgaben durchführen (weitere Informationen dazu finde Sie in der Hilfe von Kaspersky Security Center).

Das Verfahren zum Konvertieren von Richtlinien und Aufgaben ist in der Kaspersky Security Center Web Console nicht verfügbar. Wenn Sie zur Verwaltung der App die Web Console verwenden, müssen Sie neue Richtlinien und Aufgaben für die aktualisierte Version der App erstellen. Einige Parameterwerte von Richtlinien und Aufgaben können Sie aus der vorherigen Version der Richtlinien oder Aufgaben auf die neue übertragen, indem Sie Einstellungen exportieren und importieren.

In der Befehlszeile werden die Werte für die meisten Einstellungen aus der vorherigen App-Version übernommen. Sie können die App-Einstellungen auch übertragen, indem Sie die Einstellungen zunächst in eine Datei exportieren und sie anschließend aus der Datei importieren.

Einstellungen, die in der früheren App-Version nicht vorhanden sind, werden die Standardwerte angewendet. Einige Einstellungen verfügen über spezielle Werte.

Einstellungen für Ausschlüsse

Nach der Konvertierung von Aufgaben im MMC-Plug-in werden in den Untersuchungsaufgaben (z. B. vom Typ "ODS") und Aufgaben zur Untersuchung von Containern die Kontrollkästchen **Globale Ausschlüsse verwenden** und **Ausschlüsse des Schutzes vor bedrohlichen Dateien verwenden** deaktiviert. Vom Web-Plug-in wird das Konvertieren von Aufgaben nicht unterstützt.

Nach dem Aktualisieren der App über die Befehlszeile werden die Parameter `UseOASExclusions` und `UseGlobalExclusions` auf `Nein` gesetzt.

Parameter zur Verwendung von Kaspersky Security Network

Nach dem Konvertieren einer Richtlinie im MMC-Plug-in wird in den Eigenschaften der Richtlinie die Option **Kaspersky Endpoint Security nicht verwenden** ausgewählt. Vom Web-Plug-in wird das Konvertieren von Richtlinien nicht unterstützt.

Nach dem Upgrade der App über die Befehlszeile wird der Parameter `UseKSN` auf `No` gesetzt, wenn Sie beim Upgrade den Parameter `KESL_USE_KSN=No` angegeben haben. Wenn Sie `KESL_USE_KSN=Yes` angegeben haben, wird der Wert auf `UseKSN=Extended` gesetzt. Für die verbleibenden Fälle ändert sich der Wert des Parameters `UseKSN` nach dem Update nicht.

Um die Verwendung von Kaspersky Security Network zu beginnen oder fortzusetzen, müssen Sie folgendes tun:

- Wenn Sie das MMC- oder Web-Plug-in verwenden, wählen Sie die Option **Standardmäßiger KSN-Modus** oder **Erweiterter KSN-Modus** .

- Wenn Sie die Befehlszeile verwenden, setzen Sie den Wert des Parameters `UseKSN` auf `Basic` oder `Extended`.

Einstellungen für die Verwendung des Cloud-Modus

Nach dem Konvertieren einer Richtlinie im MMC-Plugin wird das Kontrollkästchen **Cloud-Modus aktivieren** deaktiviert. Vom Web-Plug-in wird das Konvertieren von Richtlinien nicht unterstützt.

Nach dem Aktualisieren der App über die Befehlszeile wird der Parameter `CloudMode` auf den folgenden Wert gesetzt:

- `CloudMode=No`, wenn nach dem Update der Parameter `UseKSN=No` eingestellt ist
- `CloudMode=Yes`, wenn nach dem Update der Parameter `UseKSN=Yes` eingestellt ist und vor dem Update der Wert `CloudMode=Yes` angegeben war.

Der Cloud-Modus ist verfügbar, wenn KSN aktiviert ist. Um den Cloud-Modus zu aktivieren, müssen Sie folgendes tun:

- Wenn Sie ein MMC- oder Web-Plugin verwenden, wählen Sie die Option **Erweiterter KSN-Modus** und aktivieren Sie das Kontrollkästchen **Cloud-Modus aktivieren**.
- Wenn Sie die Befehlszeile verwenden, geben Sie für die die Parameter `UseKSN` und `CloudMode` den Wert `Yes` an.

Modus des Interceptors von Dateioperationen

Wenn in der vorherigen Version der App das Kontrollkästchen **Zugriff auf Dateien während der Untersuchung blockieren** deaktiviert war, wird nach der Konvertierung der Richtlinie im MMC-Plug-in der Parameter **Erste Aktion** der Aufgabe zum Schutz vor bedrohlichen Dateien auf **Blockieren** gesetzt. Vom Web-Plug-in wird das Konvertieren von Richtlinien nicht unterstützt.

Der Name des Befehlszeilenparameters, der den Modus zum Abfangen von Dateioperationen festlegt, hat sich in der neuen Version der App von `InterceptorProtectionMode=Block|Notify` auf `FileBlockDuringScan=Yes|No` geändert. Wenn in einer früheren Version der App der Parameter `InterceptorProtectionMode` auf `Notify` gesetzt war, wird nach der Aktualisierung der App über die Befehlszeile der Parameter `FileBlockDuringScan` auf `No` und der Parameter `FirstAction` der Aufgabe zum Schutz vor bedrohlichen Dateien auf `Block` gesetzt.

Anwendung deinstallieren

Die Deinstallation von Kaspersky Endpoint Security besteht aus den folgenden Schritten:

1. **Deinstallation der App und der grafischen Benutzeroberfläche.**

   Wenn Sie die grafische Benutzeroberfläche verwendet haben, müssen Sie neben den App auch die grafische Benutzeroberfläche der App von den geschützten Geräten deinstallieren.

   Sie können das App-Paket und das Paket für die grafische Benutzeroberfläche gleichzeitig deinstallieren oder nur das Paket für die grafische Benutzeroberfläche deinstallieren. Es ist nicht möglich, nur das App-Paket zu deinstallieren, wenn das Paket der grafischen Benutzeroberfläche installiert ist.

   Sie können die App und die grafische Benutzeroberfläche der App auf folgende Arten löschen:

   - Per Fernzugriff über Kaspersky Security Center.
   - Lokal über die Befehlszeile.

   Während die App gelöscht wird, werden alle Aufgaben von Kaspersky Endpoint Security auf dem Gerät beendet.

2. **Administrationsagent deinstallieren**

   Wenn Sie Kaspersky Endpoint Security mithilfe von Kaspersky Security Center verwaltet haben, müssen Sie den Administrationsagenten von den geschützten Geräten entfernen.

   Sie können den Administrationsagenten auf folgende Arten deinstallieren:

   - Per Fernzugriff über Kaspersky Security Center.
   - Lokal über die Befehlszeile.

3. **Deinstallation des Verwaltungs-Plug-in für Kaspersky Endpoint Security**

   Wenn Sie Kaspersky Endpoint Security mithilfe von Kaspersky Security Center verwaltet haben, müssen Sie das Web-Plug-in oder das MMC-basierte Plug-in zur Verwaltung von Kaspersky Endpoint Security entfernen, je nachdem, welche Verwaltungskonsole Sie für Kaspersky Security Center verwendet haben.

Nach der Deinstallation der App werden alle Informationen gelöscht, die während ihrer Ausführung gespeichert wurden, mit Ausnahme der Lizenzdatenbank. Es werden zudem die installierten Zertifikate der App gelöscht. Die Lizenzdatenbank bleibt erhalten und Sie können sie für eine erneute Installation der App verwenden.

Wenn die App auf einem systemd-System installiert wurde, werden die systemd-Einstellungen nach der Deinstallation der App auf ihren ursprünglichen Zustand zurückgesetzt.

Informationen zum Deinstallieren der App und des Administrationsagenten mithilfe von Kaspersky Security Center

Sie können Kaspersky Endpoint Security und den Administrationsagenten per Fernzugriff von Client-Geräten deinstallieren.

Die Deinstallation erfolgt über die Aufgabe zur Remote-Deinstallation der App in der Kaspersky Security Center Web Console oder in der Verwaltungskonsole. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security Center.

Wenn Sie nur die grafische Benutzeroberfläche deinstallieren möchten, ohne die App zu deinstallieren, geben Sie die Einstellung `USE_GUI=No` in der Konfigurationsdatei autoinstall.ini an und starten Sie die Aufgabe zur Remote-Installation der App.

Die Deinstallation erfolgt im Hintergrund. Nach Abschluss der Deinstallation der App wird eine Aufforderung zum Neustart des Client-Geräts angezeigt.

App über die Befehlszeile löschen

App-Paket und Paket der grafischen Benutzeroberfläche deinstallieren

Um die App und die grafische Benutzeroberfläche nach einer Installation aus rpm-Paketen zu deinstallieren, führen Sie den folgenden Befehl aus:

```
# rpm -e kesl kesl-gui
```

Um die App und die grafische Benutzeroberfläche nach einer Installation aus deb-Paketen zu deinstallieren, führen Sie den folgenden Befehl aus:

```
# apt-get purge kesl kesl-gui
```

App-Paket ohne Paket der grafischen Benutzeroberfläche deinstallieren

Um die App nach einer Installation aus einem rpm-Paket ohne Deinstallation der grafischen Benutzeroberfläche zu deinstallieren, führen Sie den folgenden Befehl aus:

```
# rpm -e kesl
```

Um die App nach einer Installation aus einem deb-Paket ohne Deinstallation der grafischen Benutzeroberfläche zu deinstallieren, führen Sie den folgenden Befehl aus:

```
# apt-get purge kesl
```

Paket der grafischen Benutzeroberfläche deinstallieren

Um die grafische Benutzeroberfläche nach einer Installation aus einem rpm-Paket zu deinstallieren, führen Sie den folgenden Befehl aus:

```
# rpm -e kesl-gui
```

Um die grafische Benutzeroberfläche nach einer Installation aus einem deb-Paket zu deinstallieren, führen Sie den folgenden Befehl aus:

```
# apt-get purge kesl-gui
```

Nach Abschluss des Deinstallationsvorgangs wird eine Meldung über die Deinstallationsergebnisse angezeigt.

Administrationsagent über die Befehlszeile deinstallieren

Um einen auf einem 32-Bit-Betriebssystem aus einem rpm-Paket installierten Administrationsagenten zu deinstallieren, führen Sie den folgenden Befehl aus:

```
# rpm -e klnagent
```

Um einen auf einem 64-Bit-Betriebssystem aus einem rpm-Paket installieren Administrationsagenten zu deinstallieren, führen Sie den folgenden Befehl aus:

```
# rpm -e klnagent64
```

Um einen auf einem 32-Bit-Betriebssystem aus einem deb-Paket installierten Administrationsagenten zu deinstallieren, führen Sie den folgenden Befehl aus:

```
# apt-get purge klnagent
```

Um einen auf einem 64-Bit-Betriebssystem aus einem deb-Paket installieren Administrationsagenten zu deinstallieren, führen Sie den folgenden Befehl aus:

```
# apt-get purge klnagent64
```

Nach Abschluss des Deinstallationsvorgangs wird eine Meldung über die Deinstallationsergebnisse angezeigt.

Informationen zum Deinstallieren der Verwaltungs-Plug-ins für Kaspersky Endpoint Security

Das Web-Plug-in für die Verwaltung von Kaspersky Endpoint Security wird in der Kaspersky Security Center Web Console in der Liste der installierten Plug-ins deinstalliert (**Einstellungen** → **Web-Plug-ins**).

Um das MMC-Plug-in zu deinstallieren, verwenden Sie die Standard-Tools zum Deinstallieren von Apps im Betriebssystem. In der Liste der Apps müssen Sie **Kaspersky Endpoint Security <Versionsnummer> für Linux** zur Deinstallation auswählen.

Lizenzierung der App

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Lizenzierung der App von Kaspersky Endpoint Security verbunden sind.

Über den Endbenutzer-Lizenzvertrag

Der *Endbenutzer-Lizenzvertrag* ist ein rechtsgültiger Vertrag zwischen Ihnen und AO Kaspersky Lab. Er legt die Nutzungsbedingungen für die App fest.

Lesen Sie den Lizenzvertrag sorgfältig durch, bevor Sie mit der Verwendung der App beginnen.

Sie können die Bedingungen der Lizenzvereinbarung für Kaspersky Endpoint Security und die Datenschutzrichtlinie, in der die Verarbeitung und Übertragung von Daten beschreiben ist, auf folgende Weise einsehen:

- Durch Lesen der Datei license.<ID der Sprache>. Diese Datei gehört zum Lieferumfang des der App.
- Während der Installation der App Kaspersky Endpoint Security.

  Sie akzeptieren die Bedingungen der Lizenzvereinbarung und der Datenschutzrichtlinie, indem Sie während der Erstellung des Installationspakets für die App (bei einer Installation mit Kaspersky Security Center) oder während der Ersteinrichtung der App (bei einer Installation über die Befehlszeile) Ihre Zustimmung zu den Texten der Lizenzvereinbarung und der Datenschutzrichtlinie ausdrücken. Wenn Sie den Bedingungen der Lizenzvereinbarung und der Datenschutzrichtlinie nicht zustimmen, müssen Sie die Installation der App beenden und die Verwendung der App einstellen.

- Nach der Installation von Kaspersky Endpoint Security.

  Nach der Installation der App befinden sich Dateien mit dem Inhalt der Lizenzvereinbarung von Kaspersky Endpoint Security und der Datenschutzrichtlinie auf dem geschützten Gerät im Verzeichnis /opt/kaspersky/kesl/doc/license.<ID der Sprache>.

Über die Lizenz

Eine *Lizenz* stellt ein zeitlich begrenztes Recht zur Nutzung von Kaspersky Endpoint Security dar, das Ihnen gemäß den Bedingungen der abgeschlossenen Lizenzvereinbarung (Endbenutzer-Lizenzvertrag) gewährt wird.

Der Umfang der verfügbaren Funktionen und die Nutzungsdauer der App hängen von der Lizenz ab, mit der die App verwendet wird.

Es sind folgende Lizenztypen vorgesehen:

- *Test* – Eine kostenlose Lizenz, die zum Kennenlernen der App gedacht ist.

  Die Testlizenz besitzt eine beschränkte Gültigkeitsdauer. Nach Ablauf der Gültigkeitsdauer der Testlizenz stellt Kaspersky Endpoint Security alle Funktionen ein. Um die App weiterhin nutzen zu können, müssen Sie eine kommerzielle Lizenz erwerben.

  Sie können die App im Rahmen einer Testlizenz nur einmal für einen Testzeitraum verwenden.

- *Kommerziell* – Eine kostenpflichtige Lizenz.

  Nach Ablauf der kommerziellen Lizenz stellt die App ihre Hauptfunktionen ein. Um den Betrieb von Kaspersky Endpoint Security fortzusetzen, müssen Sie die kommerzielle Lizenz verlängern. Nach Ablauf der Lizenz können Sie die App nicht mehr verwenden und müssen sie von Ihrem Gerät entfernen.

  Es wird empfohlen, die Gültigkeitsdauer einer Lizenz spätestens zum Ablaufdatum der aktiven Lizenz zu verlängern, um einen ununterbrochenen Schutz der Geräte vor Bedrohungen zu gewährleisten.

Über das Lizenzzertifikat

Das *Lizenzzertifikat* ist ein Dokument, das Ihnen zusammen mit der Schlüsseldatei bzw. dem Aktivierungscode übergeben wird.

Ein Lizenzzertifikat enthält die folgenden Informationen über die bereitgestellte Lizenz:

- Lizenzschlüssel oder Bestellnummer
- Informationen über den Benutzer, für den die Lizenz bereitgestellt wird
- Informationen zur App, die über die bereitgestellte Lizenz aktiviert werden kann
- Beschränkung der Anzahl der Lizenzierungseinheiten (z. B. Geräte, auf denen die App mit dieser Lizenz verwendet werden darf)
- Beginn der Gültigkeitsdauer der Lizenz
- Ablaufdatum der Lizenz oder Gültigkeitsdauer der Lizenz
- Lizenztyp

Über den Lizenzschlüssel

Der *Lizenzschlüssel* ist eine Abfolge von Bits, mit deren Hilfe Sie die App aktivieren und anschließend gemäß den Bedingungen des Endbenutzer-Lizenzvertrags verwenden können. Der Lizenzschlüssel wird von Kaspersky erstellt.

Sie können auf eine der folgenden Arten einen Lizenzschlüssel zur App hinzufügen: indem Sie eine *Schlüsseldatei* anwenden oder einen *Aktivierungscode* eingeben. Sobald Sie den Lizenzschlüssel in der App hinzufügen, wird er in der Benutzeroberfläche der App als eindeutige Folge aus Buchstaben und Ziffern angezeigt.

Bei Verstößen gegen die Bedingungen des Endbenutzer-Lizenzvertrags kann der Lizenzschlüssel von Kaspersky blockiert werden. Ist der Lizenzschlüssel blockiert, so wird zur Nutzung der App ein anderer Lizenzschlüssel benötigt.

Für Kaspersky Endpoint Security sind die folgenden *Arten* von Lizenzschlüsseln verfügbar:

- *App-Schlüssel* – Ein Lizenzschlüssel zur Aktivierung der Funktionalität von Kaspersky Endpoint Security. Der Umfang an verfügbaren Funktionen der App hängt von der Lizenz ab, die dem App-Schlüssel zugeordnet ist.
- *EDR Optimum-Schlüssel* – Ein zusätzlicher Lizenzschlüssel für das Add-on von Kaspersky Endpoint Detection and Response Optimum zur Aktivierung der Funktionalität von Kaspersky Endpoint Detection and Response Optimum. Dieser Schlüssel wird benötigt, wenn Sie die App unter einer Lizenz verwenden, von der die Funktionalität von Kaspersky Endpoint Detection and Response Optimum nicht abgedeckt wird.

Ein Lizenzschlüssel kann entweder ein "aktiv" oder "Reserve" sein.

Aktiver Lizenzschlüssel – Ein Lizenzschlüssel, der aktuell für die Ausführung der App verwendet wird. Als aktiv hinzugefügt werden können: Lizenzschlüssel für Testlizenzen, Schlüssel für kommerzielle Lizenzen (kommerzieller Schlüssel) oder Schlüssel für Abonnements. Sie können der App nur einen aktiven Schlüssel jedes Typs hinzufügen.

Reserveschlüssel – Ein Lizenzschlüssel, der das Recht auf die Nutzung der App gewährt, jedoch im Augenblick nicht verwendet wird. Ein Reserveschlüssel wird automatisch zum aktiven Lizenzschlüssel, sobald die mit dem aktuellen Schlüssel verbundene Lizenz abläuft. Ein Reserveschlüssel kann nur hinzugefügt werden, wenn bereits ein aktiver Lizenzschlüssel vom gleichen Typ vorhanden ist.

Der Lizenzschlüssel einer Testlizenz kann nur als aktiver Schlüssel hinzugefügt werden. Lizenzschlüssel für eine Testlizenz oder für Abonnements können nicht als Reserve-Lizenzschlüssel hinzugefügt werden.

Über den Aktivierungscode

Ein *Aktivierungscode* besteht aus einer eindeutigen Folge von zwanzig Ziffern und lateinischen Buchstaben. Den Aktivierungscode geben Sie ein, um einen Lizenzschlüssel zur Aktivierung von Kaspersky Endpoint Security hinzuzufügen. Der Aktivierungscode wird an die E-Mail-Adresse geschickt, die Sie angegeben haben, nachdem Sie Kaspersky Endpoint Security gekauft oder eine Testversion von Kaspersky Endpoint Security angefordert haben.

Um die App mithilfe des Aktivierungscodes zu aktivieren, ist Internetzugang für die Verbindung mit den Kaspersky-Aktivierungsservern erforderlich.

Im Falle des Verlusts des Aktivierungscodes nach der Aktivierung der App setzen Sie sich bitte mit dem Partner von Kaspersky in Verbindung, von dem Sie die Lizenz erworben haben.

Über die Schlüsseldatei

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

Die Schlüsseldatei wird an die E-Mail-Adresse geschickt, die Sie angegeben haben, als Sie Kaspersky Endpoint Security gekauft oder eine Testversion von Kaspersky Endpoint Security angefordert haben.

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

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

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

- Kontaktieren Sie den Lizenzverkäufer.
- Rufen Sie die Schlüsseldatei anhand eines vorhandenen Aktivierungscodes auf der Website von Kaspersky ab.

Über das Abonnement

Ein Abonnement für die App Kaspersky Endpoint Security ist ein Kaufauftrag für die App mit bestimmten Parametern (Ablaufdatum des Abonnements, Anzahl der geschützten Geräte). Sie können ein Abonnement für die App Kaspersky Endpoint Security über Ihren Dienstanbieter (z. B. Ihren Internetprovider) bestellen. Sie können Ihr Abonnement verlängern oder kündigen. Sie können Ihr Abonnement auf der Website des Dienstanbieters verwalten.

Ein Abonnement kann beschränkt (beispielsweise auf ein Jahr) oder unbefristet (ohne Ablaufdatum) sein. Damit die App nach Ablauf des beschränkten Abonnements weiter funktioniert, müssen Sie Ihr Abonnement verlängern. Ein unbefristetes Abonnement wird automatisch verlängert, wenn die Gebühren des Händlers rechtzeitig bezahlt wurden.

Nach Ablauf eines befristeten Abonnements wird Ihnen möglicherweise eine Nachfrist zur Abonnement-Verlängerung gewährt, während der die Funktionalität der App erhalten bleibt. Ob es eine Nachfrist gibt und wie lang diese ist, wird vom Dienstanbieter bestimmt.

Die verfügbaren Optionen für die Verwaltung des Abonnements können je nach Dienstanbieter unterschiedlich sein. Ihr Dienstanbieter gewährt möglicherweise keine Nachfrist für die Verlängerung des Abonnements, innerhalb der die Funktionen der App erhalten bleiben.

Um die App Kaspersky Endpoint Security im Abonnement zu nutzen, müssen Sie den Aktivierungscode anwenden, den Sie von Ihrem Dienstanbieter erhalten. Nach der Anwendung des Aktivierungscodes wird der App ein aktiver Schlüssel hinzugefügt, welcher der Lizenz für die Verwendung der App im Abonnement entspricht. Ein Reserveschlüssel kann nur mithilfe eines Aktivierungscodes hinzugefügt werden. Das Hinzufügen mittels Schlüsseldatei oder Abonnement ist nicht möglich.

Die für ein Abonnement erhaltenen Aktivierungscodes können nicht zum Aktivieren vorheriger Versionen der App Kaspersky Endpoint Security verwendet werden.

Vergleich der App-Funktionen je nach Lizenz

Die in Kaspersky Endpoint Security verfügbaren Funktionen sind von Lizenz abhängig (s. Tabelle unten).

Vergleich der App-Funktionen der Lösung auf Basis von Prozessoren mit Intel-Architektur. Informationen zu Lizenzen und verfügbaren Funktionen der Lösung auf Basis von Prozessoren mit Arm-Architektur können erfragen Sie bitte bei einem Anbieter in Ihrer Region.

Vergleich der Funktionen der App

Funktion	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Endpoint Security for Business Total	Kaspersky Hybrid Cloud Security (Desktop)	Kaspersky Security for Virtualization (Desktop)	Kaspers Hybric Cloud Securit Enterpr (Deskto Enterpri

Schutz vor bedrohlichen Dateien	✓	✓	✓	✓	✓	✓
Schutz vor Web-Bedrohungen	✓	✓	✓	✓	✓	✓
Schutz vor Netzwerkbedrohungen	✓	✓	✓	✓	✓	✓
Firewall-Verwaltung	✓	✓	✓	✓	✓	✓
Verhaltensanalyse	✓	✓	✓	✓	✓	✓
Gerätekontrolle	✓	✓	✓	✓	✓	✓
Untersuchung von Wechseldatenträgern	✓	✓	✓	✓	✓	✓
Schutz vor Verschlüsselung (für freigegebene Ordner)	✓	✓	✓	–	–	✓
Untersuchung von Containern	–	–	–	–	–	✓
Überwachung der Systemintegrität	–	–	–	–	–	✓
App-Kontrolle	–	✓	✓	✓	✓	✓
Web-Kontrolle	✓	✓	✓	✓	✓	✓
Integration mit Kaspersky Endpoint Detection and Response Optimum	–	–	–	–	–	–

Bereitstellung von Daten

Dieser Abschnitt enthält Informationen zu den Daten, die Kaspersky Endpoint Security auf dem Gerät speichern und während seiner Ausführung automatisch an Kaspersky übertragen kann.

Kaspersky schützt alle auf diese Weise empfangenen Daten gemäß gesetzlichen Vorschriften und den geltenden Regeln von Kaspersky. Die Datenübertragung erfolgt über verschlüsselte Kommunikationskanäle.

Weitere Informationen zur Verarbeitung, Speicherung und Vernichtung der Daten, die während der Verwendung der App abgerufen und an Kaspersky übertragen werden, finden Sie in der Lizenzvereinbarung, der Erklärung zu Kaspersky Security Network und der Datenschutzrichtlinie auf der Website von Kaspersky. Die Dateien license.<ID der Sprache> und ksn_license.<ID der Sprache> enthalten den Endbenutzer-Lizenzvertrag und die Erklärung zu Kaspersky Security Network und gehören zum Lieferumfang der App.

Daten, die bei Verwendung eines Aktivierungscodes bereitgestellt werden

Wenn Kaspersky Endpoint Security im Standard-Modus verwendet wird und mit einem Aktivierungscode aktiviert wurde, stimmen Sie zu, die folgenden Informationen automatisch an Kaspersky zu übertragen, damit die rechtmäßige Nutzung der App bestätigt werden kann und Statistikdaten zur Verteilung und Verwendung der App abgerufen werden können:

- Typ, Version und Lokalisierung der installierten App
- Versionen der installierten Updates für die App
- Geräte-ID und ID der App-Installation auf dem Gerät
- Aktivierungscode, mit dem die App aktiviert ist
- ID der gültigen Lizenz
- Datum und Uhrzeit der Erstellung des Lizenzschlüssels der App
- Datum und Uhrzeit auf dem Gerät des Benutzers
- Datum und Uhrzeit des Ablaufs der Lizenz zur Verwendung der App
- Typ, Version und Bitzahl des Betriebssystems

Daten, die beim Herunterladen von Updates von den Kaspersky-Update-Servern bereitgestellt werden

Wenn Kaspersky Endpoint Security im Standard-Modus verwendet wird und wenn Sie zum Herunterladen von Updates die Kaspersky-Update-Server verwenden, stimmen Sie zu, die folgenden Informationen automatisch an Kaspersky zu übertragen, damit der Update-Vorgang effizienter ausgeführt werden kann und Statistikdaten zur Verteilung und Verwendung der App abgerufen werden können:

- von der Lizenz abgeleitete App-ID
- vollständige Version der App

- ID der App-Lizenz
- Typ der verwendeten Lizenz
- ID der App-Installation (PCID)
- ID des Starts des App-Updates
- verarbeitete Webadresse

Daten, die bei Verwendung der App im Light Agent-Modus übertragen werden

Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird (als Teil von Kaspersky Security for Virtualization Light Agent), werden von der App während der Ausführung die folgenden Informationen, die personenbezogene und vertrauliche Daten enthalten können, gespeichert und an andere Komponenten der Lösung übertragen:

- Zur Aktivierung übermittelt die Kaspersky Endpoint Security folgende Daten an den Schutzserver: die Gültigkeitsdauer der Statusbestätigung des Lizenzschlüssels: die BIOS-ID der geschützten virtuellen Maschine; Informationen über die Lizenz, die der Light Agent für seine Ausführung benötigt.
- Um die Datenbanken des Light Agent zu aktualisieren, überträgt Kaspersky Endpoint Security die folgenden Daten an den Schutzserver: aus der Lizenz abgeleitete Programm-ID; vollständige Versionsnummer des Programms; Lizenz-ID des Programms; Installations-IDs des Programms (PCID); verarbeitete Webadresse; Lizenztyp; ID des Update-Starts.
- Für sie Sicherstellung des Schutzes und während der Ausführung der Untersuchungsaufgaben überträgt Kaspersky Endpoint Security die zur Objektuntersuchung erforderlichen Informationen an den Schutzserver. Dies umfasst die Namen von Dateien und Pfade von Dateien im Dateisystem, Datei-Hashes, Webadressen sowie untersuchte Objekte oder deren Fragmente.
- In einer Infrastruktur unter Verwaltung von VMware vCenter Server und VMware NSX Manager kann Kaspersky Endpoint Security im Falle einer Erkennung von Viren, Schadsoftware oder von für Netzwerkangriffe typischen Aktivitäten die Informationen über Sicherheits-Tags, die einer geschützten virtuellen Maschine zugewiesen sind, an den Integrationsserver übermitteln. Dazu gehört auch die Übertragung der IDs von geschützten virtuellen Maschinen.
- Um Informationen abzurufen, die bei der Auswahl der zu verbindenden SVM benötigt werden, übergibt Kaspersky Endpoint Security die ID der geschützten virtuellen Maschine an den Integrationsserver und den Schutzserver.
- Bei Verwendung von Kaspersky Security for Virtualization Light Agent im Modus für Mandantenfähigkeit können die für die Erstellung von Berichten zum Schutz der Mandanten erforderlichen Informationen von Kaspersky Endpoint Security an den Schutzserver übertragen werden. Dies kann umfassen: ID der geschützten virtuellen Maschine; Typ und Version des Gastbetriebssystems auf der geschützten virtuellen Maschine; Verbindungszeiträume von Kaspersky Endpoint Security mit der SVM.
- Um Statistiken abrufen zu können, übermittelt Kaspersky Endpoint Security die folgenden Informationen an den Schutzserver: Informationen über die Version des Betriebssystems der geschützten virtuellen Maschine; Lokalisierungseinstellungen von Kaspersky Endpoint Security; Namen der aktiven Komponenten von Kaspersky Endpoint Security; ID der geschützten virtuellen Maschine (BIOS-ID).

Die angegebenen Informationen werden über verschlüsselte Datenkanäle übertragen, mit Ausnahme jener Informationen, die zur Überprüfung von Objekten erforderlich sind und die bei SVM-Auwahl verwendet werden. Die Verbindung zwischen Kaspersky Endpoint Security und den Schutzservern ist standardmäßig nicht abgesichert. Sie können die Verschlüsselung des Datenkanals zur Übertragung zwischen Light Agents und Schutzservern in den Einstellungen von Kaspersky Endpoint Security aktivieren.

Daten, die von der App an Kaspersky Security Center übertragen werden

Während der Ausführung der App Kaspersky Endpoint Security kann die App folgende Informationen, die eventuell persönliche und vertrauliche Daten enthalten, speichern und an Kaspersky Security Center weitergeben:

- Informationen zu den in der App verwendeten Datenbanken:
  - Liste der von der App benötigten Datenbank-Kategorien
  - Zeitpunkt (Datum und Uhrzeit), zu dem die verwendeten Datenbanken veröffentlicht und in die App geladen wurden
  - Erscheinungsdatum der heruntergeladenen Updates der App-Datenbanken
  - Zeitpunkt des letzten Updates der App-Datenbanken
  - Anzahl der Einträge in den aktuell verwendeten App-Datenbanken
- Informationen über die Lizenz zur Nutzung der App:
  - Seriennummer und Lizenztyp
  - Gültigkeitsdauer der Lizenz in Tagen
  - Anzahl der Geräte, auf die sich die Lizenz erstreckt
  - Datum für den Beginn und das Ende der Lizenzgültigkeit
  - Status des Lizenzschlüssels
  - Datum und Uhrzeit der letzten erfolgreichen Synchronisierung mit den Aktivierungsservern, falls die App mit einem Aktivierungscode aktiviert wurde
  - ID der App, für deren Aktivierung die Lizenz bereitgestellt wurde
  - die gemäß der Lizenz verfügbare Funktionalität
  - Name der Organisation, der die Lizenz erteilt wurde
  - zusätzliche Informationen, falls die App im Abonnement genutzt wird (Indikator für Abonnement, Ablaufdatum des Abonnementzeitraums und Anzahl der Tage, die für die Verlängerung des Abonnements zur Verfügung stehen, Webadresse des Abonnementanbieters, aktueller Status und Grund für den Wechsel zu diesem Status), Datum und Uhrzeit der Aktivierung der App auf dem Gerät
  - Datum und Uhrzeit des Ablaufs der Lizenz auf dem Gerät
- Informationen zu App-Updates:
  - Liste der Updates, die installiert oder gelöscht werden sollen

- Veröffentlichungsdatum und Vorhandensein des Status *Kritisch*
- Name, Version und kurze Beschreibung des Updates
- Link zu einem Artikel mit einer vollständigen Beschreibung des Updates
- ID und Text des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie für das App-Update
- ID und Text der Erklärung zu Kaspersky Security Network für das App-Update
- Indikator dafür, ob das Update gelöscht werden kann
- Versionen der Richtlinie und des Verwaltungs-Plug-ins für die App
- Webadresse zum Herunterladen des Verwaltungs-Plug-in für die App
- Namen der installierten App-Updates, Version und Datum ihrer Installation
- Fehlercode und Beschreibung des Fehlers, falls die Installation oder das Löschen des Updates mit einem Fehler beendet wurde
- Anzeichen und Ursache für die Notwendigkeit eines Neustarts des Geräts oder der App im Rahmen eines App-Updates

- Zustimmung oder Ablehnung der Bedingungen der Erklärung zu Kaspersky Security Network, des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie durch den Benutzer
- Liste der dem Gerät zugewiesenen Tags
- Liste der Statuszustände des Geräts und Gründe für deren Zuweisung.
- Allgemeiner Status der App und Status aller ihrer Komponenten; Informationen zur Einhaltung von Richtlinien; Status des Echtzeitschutzes des Geräts; Status der Anwendungsstabilität; Informationen über Unterbrechungen der App-Ausführung.
- Datum und Uhrzeit der letzten Untersuchung des Geräts; Anzahl der untersuchten Objekte; Anzahl der erkannten schädlichen Objekte; Anzahl der blockierten, gelöschten und desinfizierten Objekte; Anzahl der Objekte, die nicht desinfiziert werden konnten; Anzahl der Untersuchungsfehler; Anzahl der erkannten Netzwerkangriffe
- Daten zu den derzeit angewendeten Werten der App-Einstellungen
- Aktueller Status und Ergebnis der Ausführung von Gruppenaufgaben und lokalen Aufgaben sowie die Werte ihrer Einstellungen
- Informationen zu externen Geräten, die an das Client-Gerät angeschlossen sind (ID, Name, Typ, Hersteller, Beschreibung, Seriennummer und VID/PID)
- Informationen zu Backup-Kopien von Dateien, die im Backup gespeichert sind (Name, Pfad, Größe und Typ des Objekts, Beschreibung des Objekts, Name der erkannten Bedrohung, Version der App-Datenbanken, mit denen die Bedrohung erkannt wurde, Zeitpunkt (Datum und Uhrzeit), zu dem das Objekt in den Backup verschoben wurde, Aktionen für das Objekt im Backup (gelöscht, wiederhergestellt)) sowie die eigentlichen Dateien auf Anfrage des Administrators
- Informationen über den Betrieb jeder App-Komponente und die Ausführung jeder Aufgabe in Form von Ereignissen:

- Datum und Uhrzeit des Ereignisses
- Name und Typ des Ereignisses
- Ereigniskategorie
- Name der Aufgabe oder Komponente der App, bei deren Ausführung das Ereignis eingetreten ist
- Informationen zu der App, die ein Ereignis verursacht hat: Name der App, Pfad der Datei auf der Festplatte, Prozess-ID, Werte der Einstellungen, falls das Ereignis sich auf den App-Start oder die Änderung der Betriebseinstellungen bezieht
- Benutzer-ID
- Name des Initiators (Aufgabenplanung, App-Name, Kaspersky Security Center oder Benutzername), dessen Aktionen das Ereignis verursacht haben
- Name und ID des Benutzers, der den Zugriff auf die Datei initiiert hat
- Ergebnis der Verarbeitung eines Objekts oder einer Aktion (Beschreibung, Typ, Name, Bedrohungsstufe und Genauigkeit, Dateiname und Art des Vorgangs auf dem Gerät, Entscheidung der App für diesen Vorgang)
- Informationen zum Objekt (Name und Typ des Objekts, Pfad zum Objekt auf der Festplatte, Version des Objekts, Größe, Informationen zur durchgeführten Aktion, Beschreibung der Ursache für das Ereignisses, Beschreibung der Ursache für die Nichtverarbeitung und das Überspringen des Objekts)
- Informationen über das Gerät (Herstellername, Gerätename, Pfad, Gerätetyp, Bustyp, ID, VID/PID, Systemgerätezeichen, Name des Regelplans für den Gerätezugriff)
- Informationen zum Sperren und Entsperren des Geräts; Informationen zu blockierten Verbindungen (Name, Beschreibung, Gerätename, Protokoll, Remote-Adresse und Port, lokale Adresse und Port, Paketregeln, Aktionen)
- Informationen über die angeforderte Webadresse
- Informationen über erkannte Objekte
- Typ, Methode und ID der Erkennung
- Informationen über die durchgeführte Aktion
- Informationen zu den App-Datenbanken (Veröffentlichungsdatum der heruntergeladenen Datenbanken-Updates, Informationen zur Anwendung der Datenbanken, Fehler bei der Anwendung der Datenbanken, Informationen zur Außerkraftsetzung der installierten Datenbanken-Updates)
- Informationen zur Erkennung von Verschlüsselung (Name der Ransomware; Name des Geräts, auf dem die Verschlüsselung erkannt wurde; Informationen zum Sperren und Entsperren des Geräts)
- App-Einstellungen und Netzwerkeinstellungen
- Informationen über die ausgelöste Regel für die App-Kontrolle (Name und Typ) und das Ergebnis ihrer Anwendung
- Informationen zu Containern (Namen von Containern oder Container-Images, Pfade zu Containern oder Container-Images, Web-Adressen von Repositories)
- Informationen zu aktiven und blockierten Verbindungen (Name, Beschreibung und Typ)

- Informationen zum Blockieren und Entsperren des Zugriffs auf nicht vertrauenswürdige Geräte
- Informationen über die Nutzung von KSN (Verbindungsstatus mit KSN, KSN-Infrastruktur, ID der KSN-Erklärung im erweiterten Modus, Akzeptanz der KSN-Erklärung im erweiterten Modus, ID der KSN-Erklärung, Akzeptanz der KSN-Erklärung)
- Informationen zu Zertifikaten (Domänenname, Name des Antragstellers, Name des Herausgebers, Ablaufdatum, Status des Zertifikats, Typ des Zertifikats, Zeitpunkt des Hinzufügen des Zertifikats, Veröffentlichungsdatum, Seriennummer, SHA256-Fingerabdruck)
- Informationen über externe Systeme, die Teil von Unternehmenssoftwarelösungen sind (Adresse des Integrationsservers)
- Informationen über das Aktivieren und Deaktivieren der Netzwerkisolation des Geräts
- Informationen zur Ausführung im Light Agent-Modus: Name der Vorlage der virtuellen Maschine, Adresse des Integrationsservers
- Name des Geräts, für das die Netzwerkisolation aktiviert oder deaktiviert ist
- Statistiken zur Ausführung der Untersuchungsaufgaben: Anzahl der untersuchten Objekte; Anzahl der erkannten Bedrohungen; Anzahl infizierter Objekte; Anzahl möglicherweise infizierter Objekte; Anzahl desinfizierter Objekte; Anzahl der zum Backup-Speicher hinzugefügten Objekte; Anzahl gelöschter Objekte; Anzahl der Objekte, deren Desinfektion fehlschlug; Anzahl der Untersuchungsfehler; Anzahl kennwortgeschützter Objekte; Anzahl übersprungener Objekte; Anzahl der untersuchten Container und Images.
- Informationen über die Version der von der App verwendeten Komponente "EDR Optimum".
- Informationen zu Entwicklungsketten von Bedrohungen: Netzwerkname; Liste der Entwicklungsketten der Bedrohungen, ID der Entwicklungskette der Bedrohung.

- Informationen zur Ausführung der Aufgabe zur Prüfung der System-Integrität (Name, Typ, Pfad) und Informationen zur Baseline
- Informationen zu Netzwerkaktivität, Paketregeln und Netzwerkangriffen
- Informationen zur Benutzerrolle:
  - Name und ID des Benutzers, der die Änderung der Benutzerrolle initiiert hat
  - Benutzerrolle
  - Name des Benutzers, dem die Rolle zugewiesen oder entzogen wurde
- Informationen zu ausführbaren Dateien von Anwendungen, die auf dem Client-Gerät gefunden wurden (Name, Pfad, Typ und Hash der Datei; Liste der Kategorien, zu denen die App gehört; KL-Kategorien, zu der die App gehört; Zeitpunkt, zu dem die Datei erstmals gestartet wurde; Vertrauensgruppe, zu der die App gehört; Name und Version der App; Name des App-Herstellers; Informationen zu dem Zertifikat, mit dem die App signiert ist: Seriennummer, Fingerabdruck, Herausgeber, Betreff, Ausstellungsdatum, Ablaufdatum und öffentlicher Schlüssel)
- Informationen zur Netzwerkliste der Entwicklungsketten der Bedrohung: ID der Entwicklungskette der Bedrohung, Zeitpunkt der Erstellung der Entwicklungskette der Bedrohung (als Zeitstempel), Format der Entwicklungskette der Bedrohung (Text oder Archiv), Body-Größe in Bytes der Entwicklungskette der Bedrohung.

Daten, die beim Klicken auf Links von der App-Oberfläche bereitgestellt werden

Indem Sie auf einen Link in der Benutzeroberfläche der App Kaspersky Endpoint Security klicken, erklären Sie sich damit einverstanden, die folgenden Informationen automatisch an Kaspersky zu übermitteln:

- vollständige Version der App
- Lokalisierung der App
- App-ID (PID)
- Name des Links

Daten, die bei der Verwendung von Kaspersky Security Network bereitgestellt werden

Wenn Sie Kaspersky Security Network im erweiterten Modus verwenden, stimmen Sie zu, alle Informationen, die in der Erklärung zu Kaspersky Security Network aufgelistet sind, automatisch an Kaspersky zu übermitteln. Außerdem können auch Dateien (oder Dateiteile) an Kaspersky gesendet werden, die von Angreifern zur Beschädigung des Geräts und der in seinem Betriebssystem gespeicherten Daten verwendet werden können.

Die Datei ksn_license.<ID der Sprache> mit dem Text der Erklärung zu Kaspersky Security Network ist im Lieferumfang der App enthalten.

Daten, die bei der Verwendung von Kaspersky Endpoint Detection and Response Optimum bereitgestellt werden

Daten, die zusammen mit den Ergebnissen der Aufgaben zur *IoC-Untersuchung* übertragen werden

Kaspersky Endpoint Security überträgt automatisch Daten über die Ergebnisse von Aufgaben zur *IoC-Untersuchung* an Kaspersky Security Center.

Die Ergebnisdaten von Aufgaben zur *IoC-Untersuchung* können die folgenden Informationen enthalten:

- Netzwerkinformationen:
  - IP-Adresse aus der Tabelle des Protokolls zur Adressauflösung (Address Resolution Protocol – ARP)
  - MAC-Adresse aus der Tabelle des Protokolls zur Adressauflösung
  - Typ und Name des DNS-Eintrags
  - IP-Adresse des geschützten Geräts
  - MAC-Adresse des geschützten Geräts

    - IP-Adresse und Port der Remote-Verbindung
    - IP-Adresse des lokalen Netzwerkadapters
    - Nummer des offenen Ports auf dem lokalen Adapter
    - Protokollnummer gemäß dem Standard der Internet Assigned Numbers Authority (IANA)
- Informationen über Prozesse:
    - Name des Prozesses
    - Argumente des Prozesses
    - Pfad zur ausführbaren Datei des Prozesses
    - Prozess-ID (PID)
    - ID des übergeordneten Prozesses (PPID)
    - Name des Benutzers, der den Prozess gestartet hat
    - Datum und Uhrzeit des Starts des Prozesses
- Informationen über Dienste:
    - Name des Dienstes
    - Beschreibung des Dienstes
    - Pfad und Name der ausführbaren Datei des Dienstes
    - ID des Dienstes
    - Typ des Dienstes (Kernel-Treiber, Adapter usw.)
    - Status des Dienstes
    - Startmodus des Dienstes
    - Name des Benutzers, unter dem der Dienst gestartet wurde
- Informationen über das Dateisystem:
    - Name der Partition
    - Buchstabe der Partition
    - Typ der Partition
- Informationen über das Betriebssystem:
    - Name und Version des Betriebssystems
    - Netzwerkname des geschützten Geräts

- Domäne oder Gruppe, der das Gerät zugehörig ist

- Informationen über Web-Aktivitäten:
  - Name des Browsers
  - Version des Browsers
  - Zeitpunkt des letzten Zugriffs auf eine Webressource
  - Web-Adresse der HTTP-Anfrage
  - Name des Benutzers, der die HTTP-Anfrage gestellt hat
  - Name des Prozesses, der die HTTP-Anfrage gestellt hat
  - Pfad zur ausführbaren Datei des Prozesses, der die HTTP-Anfrage gestellt hat
  - ID des Prozesses, der die HTTP-Anfrage gestellt hat
  - Webadresse der Quelle der HTTP-Anfrage
  - Webadresse der angeforderten Ressource
  - Benutzeragent zur Verarbeitung von Webanfragen (HTTP User-Agent)
  - Ausführungszeit der HTTP-Anfrage
  - Die eindeutige Kennung des Prozesses, der die HTTP-Anfrage gestellt hat.

Daten zum Aufbau der Entwicklungskette der Bedrohung

Daten zum Aufbau einer Entwicklungskette der Bedrohung können die folgenden Informationen enthalten:

- Allgemeine Informationen zum dem Alarm:
  - Datum und Uhrzeit des Alarms
  - Objektname
  - Untersuchungsmodus
  - Status der letzten Aktivität mit Bezug auf den Alarm
  - Grund für eine fehlgeschlagene Verarbeitung des Alarms
- Informationen zum verarbeiteten Objekt:
  - ID des Prozesses
  - ID des übergeordneten Prozesses
  - Datei-ID des Prozesses
  - Befehl (aus der Befehlszeile) des Prozesses

- Name des Benutzers, der den Prozess gestartet hat
- ID der Sitzung, in welcher der Prozess ausgeführt wird
- Typ der Sitzung, in welcher der Prozess ausgeführt wird
- Integritätsstufe des verarbeiteten Prozesses
- Mitgliedschaft des Benutzers in privilegierten Gruppen
- ID des verarbeiteten Objekts
- Vollständiger Name des verarbeiteten Objekts
- ID des geschützten Geräts
- Vollständiger Name des Objekts (lokale Datei oder Webadresse)
- MD5- und SHA256-Hashsummen des verarbeiteten Objekts
- Typ des verarbeiteten Objekts
- Datum der Erstellung und letzten Änderung des Objekts
- Größe des zu verarbeitenden Objekts
- Attribute des verarbeiteten Objekts
- Informationen über die signierende Organisation des Objekts
- Resultat der Überprüfung des digitalen Zertifikats des Objekts
- Sicherheits-ID (SID) des Objekts
- ID der Zeitzone des Objekts
- Webadresse für den Download des Objekts (nur für Dateien)
- Name der Anwendung, von der die Datei heruntergeladen wurde
- MD5- und SHA256-Hashsummen der Anwendung, von der die Datei heruntergeladen wurde
- Name der Anwendung, von der die Datei das letzte Mal geändert wurde
- MD5- und SHA256-Hashsummen der Anwendung, von der die Datei das letzte Mal geändert wurde
- Anzahl der Starts des verarbeiteten Objekts
- Datum und Uhrzeit des ersten Starts des Objekts
- Eindeutige Datei-ID
- Vollständiger Name der Datei (lokale Datei oder Webadresse)
- Webadresse der verarbeiteten Webanfrage

- Links-Quelle der bearbeiteten Webanfrage (HTTP referer)
- Benutzeragent der verarbeiteten Webanfrage
- Typ der verarbeiteten Webanfrage (GET oder POST)
- Lokaler IP-Port für die verarbeitete Webanfrage
- Remote-IP-Port der verarbeiteten Webanfrage
- Richtung der Verbindung für die verarbeiteten Webanfrage (eingehend oder ausgehend)
- ID des Prozesses, in den der Schadcode eingeschleust wurde

Konzept der App-Verwaltung

Zur Verwaltung von Kaspersky Endpoint Security können Sie Folgendes verwenden:

- Kaspersky Security Center;
- Befehlszeile;
- grafische Benutzeroberfläche.

> Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, kann die App nicht über die Kaspersky Security Center Cloud Console und die grafische Benutzeroberfläche verwaltet werden.

Der Umfang an Aktionen, die Sie über die grafische Benutzeroberfläche von Kaspersky Endpoint Security ausführen können, ist begrenzt.

In diesem Abschnitt werden die Besonderheiten der App-Verwaltung über Kaspersky Security Center und die Befehlszeile sowie grundlegende Techniken für die Ausführung der App in den Verwaltungskonsolen von Kaspersky Security Center und der Befehlszeile beschrieben.

App mithilfe von Kaspersky Security Center verwalten

Mit Kaspersky Security Center können Sie die Ausführung von Kaspersky Endpoint Security auf Client-Geräten per Fernzugriff und zentral verwalten. Sie können Kaspersky Endpoint Security per Fernzugriff installieren und deinstallieren, starten und beenden, die Einstellungen, einzelne Komponenten und Aufgaben der App anpassen sowie Aufgaben auf den verwalteten Geräten starten und beenden.

Um Kaspersky Endpoint Security über Kaspersky Security Center zu verwalten, können Sie die folgenden Verwaltungskonsolen von Kaspersky Security Center verwenden:

- Kaspersky Security Center Verwaltungskonsole (im Folgenden auch "Verwaltungskonsole" genannt). Diese Konsole ist ein Snap-in für Microsoft Management Console (MMC), das auf dem Administrator-Arbeitsplatz installiert wird und eine Benutzeroberfläche für die Administrationsdienste des Administrationsservers und Administrationsagenten bietet.

  Die Schnittstelle zur Verwaltung von Kaspersky Endpoint Security über die Kaspersky Security Center Verwaltungskonsole wird vom MMC-Verwaltungs-Plug-in für die MMC-basierte Verwaltungskonsole (im Folgenden auch „MMC-Plug-in“ genannt) bereitgestellt.

  > In dieser Hilfe wird die Arbeit mit der Verwaltungskonsole von Kaspersky Security Center 14.2 Windows beschrieben.

- Kaspersky Security Center Web Console (im Folgenden auch "Web Console" genannt). Dabei handelt es sich um eine Webschnittstelle zur Verwaltung eines Schutzsystems auf der Basis von Kaspersky-Apps. Kaspersky Security Center Web Console kann im Browser eines jeden Geräts, welches Zugriff auf den Administrationsserver hat, aufgerufen werden.

  Die Schnittstelle zur Verwaltung von Kaspersky Endpoint Security über die Kaspersky Security Center Web Console wird vom Web-Verwaltungs-Plug-in (im Folgenden auch "Web-Plug-in" genannt) bereitgestellt.

In dieser Hilfe wird die Arbeit mit der Web Console von Kaspersky Security Center 15.1 Linux beschrieben.

- Kaspersky Security Center Cloud Console Dabei handelt es sich um eine Cloud-Verwaltungskonsole als Teil der Cloud-Version von Kaspersky Security Center, die auch Kaspersky Security Center Cloud Console genannt wird. Die Benutzeroberfläche dieser Cloud-Konsole entspricht der Benutzeroberfläche der Kaspersky Security Center Web Console. Die Schnittstelle zur Verwaltung von Kaspersky Endpoint Security über Kaspersky Security Center Cloud Console wird ebenfalls vom Web-Plug-in bereitgestellt.

  Von Kaspersky Security Center Cloud Console wird die Verwaltung der Einstellungen für die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response (KATA) nicht unterstützt.

  Die App-Verwaltung mit Kaspersky Security Center Cloud Console ist nicht verfügbar, wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird.

Mit dem MMC-Plug-in und dem Web-Plug-in können Sie in Kaspersky Security Center Richtlinien und Aufgaben erstellen, um die Ausführung von Kaspersky Endpoint Security zu verwalten:

- Eine *Richtlinie* ist eine Reihe von Einstellungen, die auf alle Geräte in der Administrationsgruppe angewendet werden. Mithilfe von Richtlinien können Sie die App-Ausführung auf allen Client-Geräten, die zur Administrationsgruppe gehören, einheitlich konfigurieren.

  Die Richtlinie für Kaspersky Endpoint Security definiert die allgemeinen Einstellungen für die Ausführung von Kaspersky Endpoint Security und die Einstellungen für die Ausführung einzelner Funktionskomponenten der App auf Geräten, auf denen die Richtlinie angewendet wird.

- *Aufgaben* für Kaspersky Endpoint Security, die in Kaspersky Security Center erstellt werden, werden auf geschützten Geräten ausgeführt und implementieren Funktionen von Kaspersky Endpoint Security wie Untersuchung auf Befehl, App-Aktivierung sowie Update der Datenbanken und Module der App.

  In Kaspersky Security Center können Sie Aufgaben erstellen, die auf einem einzelnen Gerät ausgeführt werden sollen (lokale Aufgaben), sowie Aufgaben für alle Geräte in der Administrationsgruppe (Gruppenaufgaben) oder Aufgaben für eine zufällige Auswahl von Geräten (Aufgaben für Gerätegruppen).

Unabhängig von der Verwaltungskonsole von Kaspersky Security Center, mit der Sie die Ausführung der auf Geräten installierten App Kaspersky Endpoint Security über Kaspersky Security Center verwalten, müssen Sie diese Geräte in Administrationsgruppen einordnen. Die Administrationsgruppen können Sie in Kaspersky Security Center vor der Installation von Kaspersky Endpoint Security anlegen, und anschließend Regeln zum automatischen verschieben von Geräten in die Administrationsgruppe erstellen. Alternativ können Sie die Geräte nach der Installation von Kaspersky Endpoint Security manuell in Administrationsgruppen verschieben (Weitere Informationen finden Sie in der Dokumentation von Kaspersky Security Center).

Über die Verwaltungs-Plug-ins für Kaspersky Endpoint Security

Zur Verwaltung von Kaspersky Endpoint Security über Kaspersky Security Center müssen Sie die folgenden Verwaltungs-Plug-ins installieren:

- Das Web-Plug-in für die Verwaltung von Kaspersky Endpoint Security (im Weiteren auch *Web-Plug-in*) gewährleistet die Interaktion zwischen der App Kaspersky Endpoint Security und der App Kaspersky Security Center über die Kaspersky Security Center Web Console und die Kaspersky Security Center Cloud Console.

Das Web-Plug-in muss auf dem Gerät mit installierter App Kaspersky Security Center Web Console installiert werden. Die Verwaltung von Kaspersky Endpoint Security über ein Web-Plug-in steht allen Administratoren zur Verfügung, die über einen Browser auf die Kaspersky Security Center Web Console zugreifen können.

- Das mmc-Verwaltungs-Plug-in für Kaspersky Endpoint Security (im Weiteren auch *mmc-Plug-in*) gewährleistet die Interaktion zwischen der App von Kaspersky Endpoint Security und Kaspersky Security Center über die Verwaltungskonsole.

  Das MMC-Plugin muss auf einem Gerät installiert werden, auf dem die Kaspersky Security Center Verwaltungskonsole installiert ist.

Mit den Verwaltungs-Plug-ins für Kaspersky Endpoint Security können Sie Kaspersky Endpoint Security mithilfe von Richtlinien und Aufgaben verwalten.

Nähere Informationen den Verwaltungs-Plug-ins finden Sie in der Dokumentation zu Kaspersky Security Center.

Über die Richtlinien von Kaspersky Security Center

Eine *Richtlinie* ist eine Reihe von Einstellungen für Kaspersky Endpoint Security, die auf allen Client-Geräten angewendet werden, die zu einer Administrationsgruppe gehören.

Für eine einzelne App können mehrere Richtlinien mit verschiedenen Werten eingerichtet werden. Allerdings kann innerhalb einer Administrationsgruppe nur eine einzige aktive Richtlinie für eine App gelten. Wenn Sie eine neue Richtlinie erstellen, werden alle anderen Richtlinien innerhalb einer Administrationsgruppe inaktiv. Der Status einer Richtlinie kann zu einem späteren Zeitpunkt angepasst werden.

Genau wie Administrationsgruppen unterliegen auch Richtlinien einer Hierarchie. Standardmäßig erbt eine untergeordnete Richtlinie die Einstellungen der übergeordneten Richtlinie. Eine *untergeordnete Richtlinie* ist eine Richtlinie der untergeordneten Hierarchieebene, d. h. eine Richtlinie für verschachtelte Administrationsgruppen und untergeordnete Administrationsserver. Die Vererbung von Einstellungen aus der übergeordneten Richtlinie kann deaktiviert werden.

Sie können die durch die Richtlinie festgelegten Einstellungen lokal für einzelne Geräte der Administrationsgruppe anpassen, wenn die Änderung dieser Einstellungen nicht durch die Richtlinie verboten ist.

Die Verwendung von Richtlinienprofilen ermöglicht eine flexiblere Anpassung der Einstellungen für die Ausführung der App. Ein *Richtlinienprofil* kann Einstellungen enthalten, die sich von den Einstellungen der zugrunde liegenden Richtlinie unterscheiden und die bei Erfüllung der von Ihnen festgelegten Bedingungen (den Aktivierungsregeln) auf die Client-Geräte angewendet werden. Die Verwendung von Richtlinienprofilen ermöglicht eine flexiblere Anpassung der Einstellungen auf verschiedenen Geräten. Die Profile können Sie in den Eigenschaften der Richtlinie im Abschnitt **Richtlinienprofile** erstellen und anpassen.

Jede Richtlinieneinstellung verfügt über das Attribut "Schloss", welches anzeigt, ob das Ändern der Einstellungen in untergeordneten Richtlinien und lokalen App-Einstellungen verboten ist. Die Möglichkeit zum Ändern eines Richtlinienparameters auf dem Client-Gerät wird durch den Status des "Schlosses" angezeigt, das sich bei dem Parameter in den Eigenschaften der Richtlinie befindet:

- Wenn eine Einstellung mit einem "Schloss" gesperrt ist (🔒), bedeutet dies, dass Sie den Wert der Einstellung nicht lokal oder in Richtlinien der untergeordneten Hierarchieebene anpassen können. Für alle Client-Geräte der Administrationsgruppe und untergeordnete Gruppen wird die von der Richtlinie festgelegte Einstellung verwendet.

- Wenn eine Einstellung nicht mit einem "Schloss" gesperrt ist (🔓), bedeutet dies, dass Sie den Wert der Einstellung lokal oder in Richtlinien der untergeordneten Hierarchieebene anpassen können. Wenn für Client-Geräte einer Administrationsgruppe die Einstellungen lokal oder in Richtlinien der untergeordneten Hierarchieebene festgelegt werden, wird die in den Eigenschaften der Richtlinie angegebene Einstellung nicht angewendet.

Im Web-Plugin und im MMC-Plug-in ist die Anzahl an Einstellungen, die durch ein "Schloss" gesperrt werden können, unterschiedlich. Das Web-Plug-in enthält "abschließbare" Einstellungen, die im MMC-Plug-in nicht vorhanden sind.

Die Einstellungen für die Ausführung der App werden nach der ersten Anwendung der Richtlinie gemäß den Einstellungen der Richtlinie geändert.

Weitere Informationen zu Richtlinien und Richtlinienprofilen finden Sie in der Hilfe zu Kaspersky Security Center.

Über die Aufgaben für Kaspersky Endpoint Security, die in Kaspersky Security Center erstellt wurden

Sie können in Kaspersky Security Center die folgenden Arten von Aufgaben für Kaspersky Endpoint Security erstellen:

- lokale Aufgaben zur Ausführung auf einzelnen Geräten;
- Gruppenaufgaben zur Ausführung auf Geräten, die zur Administrationsgruppe gehören;
- Aufgaben für Gerätegruppen, die auf mehreren Geräten ausgeführt werden sollen, unabhängig von deren Zugehörigkeit zu Administrationsgruppen.

  Aufgaben für bestimmte Geräte werden nur auf den Geräten ausgeführt, die in den Aufgabeneinstellungen angegeben sind. Wenn zu den bestimmten Geräten, für die eine Aufgabe erstellt wurde, neue Geräte hinzugefügt werden, so wird diese Aufgabe für diese Geräte nicht übernommen. In einem solchen Fall müssen Sie eine neue Aufgabe erstellen oder die Einstellungen der bestehenden Aufgabe bearbeiten.

Sie können beliebig viele Gruppenaufgaben, Aufgaben für bestimmte Geräte und lokale Aufgaben erstellen.

Aufgaben werden ausgeführt, wenn auf den Geräten Kaspersky Endpoint Security ausgeführt wird.

Allgemeine Informationen zu den Aufgaben, die in Kaspersky Security Center erstellt wurden, finden Sie in der Dokumentation zu Kaspersky Security Center.

Zur Verwaltung von Kaspersky Endpoint Security in Kaspersky Security Center sind die folgenden Aufgaben vorgesehen:

- **Schadsoftware-Untersuchung**. Während der Ausführung dieser Aufgabe untersucht die App die in den Aufgabeneinstellungen angegebenen Bereiche des Geräts auf Viren und andere Schadsoftware.
- **Untersuchung wichtiger Bereiche**. Während der Ausführung dieser Aufgabe untersucht die App die Bootsektoren, die Autostart-Objekte, den Prozess-Speicher und den Kernelspeicher.
- **Untersuchung von Containern**. Während der Ausführung dieser Aufgabe untersucht die App Container und Images auf Viren und andere Schadsoftware.
- **Inventarisierung**. Während der Ausführung dieser Aufgabe ruft die App Informationen über alle ausführbaren Dateien der App ab, die auf den Geräten gespeichert sind.
- **Überwachung der System-Integrität**. Während der Ausführung dieser Aufgabe registriert die App Änderungen in jedem Objekt, indem es den aktuellen Status des überwachten Objekts mit dem Originalstatus vergleicht, der zuvor als Baseline festgelegt wurde.

- **Schlüssel hinzufügen**. Während der Ausführung dieser Aufgabe wird von der App der aktive bzw. der Reserveschlüssel zur Aktivierung der App hinzugefügt.
- **Update**. Während der Ausführung dieser Aufgabe aktualisiert die App die Datenbanken entsprechend den festgelegten Update-Einstellungen.
- **Rollback des Datenbanken-Updates**. Während der Ausführung dieser Aufgabe führt die App ein Rollback des letzten Datenbanken-Updates durch.

Die Auswahl von Einstellungen sowie die Standardwerte der Aufgaben sind abhängig vom Typ der Lizenz. Die Aufgaben "Schlüssel hinzufügen", "Update" und "Rollback des Datenbanken-Updates" sind nicht anwendbar, wenn die App im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird. Außerdem werden innerhalb eines KESL-Containers einige Funktionen der App nicht unterstützt.

An Web Console und Cloud Console an- und abmelden

Kaspersky Security Center Web Console

Um sich an der Web Console anmelden zu können, müssen Sie die während der Installation von Web Console angegebene Webadresse des Administrationsservers und den Port kennen (der Standard-Port ist 8080). Außerdem muss in Ihrem Browser JavaScript aktiviert sein.

So melden Sie sich an der Web Console an:

1. Wechseln Sie in Ihrem Browser zu der Adresse `<Webadresse des Administrationsservers>:<Portnummer>`.

   Die Anmeldeseite wird angezeigt.

2. Geben Sie den Benutzernamen und das Kennwort Ihres Benutzerkontos ein.

   Es wird empfohlen, sicherzustellen, dass die Passwortkomplexität und die Anti-Brute-Force-Mechanismen gewährleisten, dass das Passwort innerhalb von 6 Monaten nicht geknackt werden kann.

3. Klicken Sie auf **Anmelden**.

   Wenn der Administrationsserver nicht antwortet oder wenn Sie ungültige Anmeldedaten eingegeben haben, wird eine Fehlermeldung angezeigt.

Nach der Anmeldung wird das Dashboard in der Sprache und dem Farbschema angezeigt, das Sie zuletzt verwendet haben.

Nähere Informationen über die Benutzeroberfläche von Web Console finden Sie in der Dokumentation zu Kaspersky Security Center.

So melden Sie sich von der Web Console ab:

Klicken Sie in der unteren linken Ecke des Bildschirms auf **<Kontoname>** → **Beenden**.

Web Console wird beendet und die Anmeldeseite wird angezeigt.

Kaspersky Security Center Cloud Console

Verwenden Sie für die Kaspersky Security Center Cloud Console ein Web-Token, um sich in Ihrem Benutzerkonto im Portal der Cloud Console anzumelden.

Detaillierte Informationen zur Kaspersky Security Center Cloud Console finden Sie in der Dokumentation zur Kaspersky Security Center Cloud Console

Richtlinienverwaltung in Web Console

Für Richtlinien stehen folgende Aktionen in der Web Console zur Verfügung:

- Richtlinie erstellen
- Richtlinieneinstellungen ändern

  > Wenn das Benutzerkonto, mit dem der Zugriff auf den Administrationsserver erfolgt, nicht zum Bearbeiten von Einstellungen einzelner Funktionsbereiche berechtigt ist, können die Einstellungen dieser Funktionsbereiche nicht bearbeitet werden. Außerdem wird die Konfiguration einiger Einstellungen im KESL-Container nicht unterstützt.

- Richtlinieneinstellungen exportieren und importieren
- Richtlinie kopieren und verschieben
- Richtlinie löschen
- Status der Richtlinie ändern
- Richtlinienprofile erstellen

Allgemeine Informationen zur Verwendung von Richtlinien finden Sie in der Hilfe zu Kaspersky Security Center.

Richtlinienerstellung in der Web Console

So erstellen Sie eine Richtlinie in der Web Console:

1. Wählen Sie im Hauptfenster von Web Console **Assets (Geräte)** → **Richtlinien und Richtlinienprofile**.

   Die Liste mit Richtlinien und Richtlinienprofilen wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die die Geräte enthält, für welche die Richtlinie angewendet werden soll. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** oberhalb der Liste der Richtlinien und Richtlinienprofile und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

3. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Richtlinien wird gestartet.

4. Wählen Sie im nächsten Fenster **Kaspersky Endpoint Security 12.1 für Linux** aus der Liste aus.

   Wechseln Sie zum nächsten Schritt des Assistenten.

5. Geben Sie an, in welchem Modus Sie Kaspersky Endpoint Security verwenden:

   - **Standard-Modus zum Schutz von Workstations und Servern** – Die App wird zum Schutz von Geräten verwendet, auf denen Linux-Betriebssysteme ausgeführt werden.

   - **Light Agent-Modus zum Schutz virtueller Umgebungen** – Die App wird im Rahmen von Kaspersky Security for Virtualization Light Agent zum Schutz virtueller Maschinen verwendet, auf denen Linux-Gastbetriebssysteme ausgeführt werden.

6. Wenn Sie die App im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, konfigurieren Sie die Einstellungen zur SVM-Ermittlung:

   a. Wählen Sie die Methode aus, die von den Light Agents verwendet werden soll, um für verfügbare SVMs zum Herstellen einer Verbindung zu erkennen:

      - **Integrationsserver verwenden**

        Wenn diese Option ausgewählt ist, stellt der Light Agent eine Verbindung zum Integrationsserver her, um eine Liste der für die Verbindung verfügbaren SVMs und Informationen darüber zu erhalten.

      - **Manuell hinzugefügte Liste mit SVM-Adressen verwenden**

        Wenn diese Option ausgewählt ist, können Sie eine Liste von SVMs angeben, mit denen Light Agents, die durch diese Richtlinie verwaltet werden, eine Verbindung herstellen können. Die Light Agents stellen nur Verbindungen zu den in der Liste angegebenen SVMs her.

      Wenn Sie die Option **Manuell hinzugefügte Liste mit SVM-Adressen verwenden** ausgewählt haben und für den Light Agent der erweiterte Algorithmus zur SVM-Auswahl verwendet wird sowie auf der SVM der Modus zum Schutz großer Infrastrukturen aktiviert ist (mehr dazu finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent), dann ist die Verbindung eines Light Agents mit dieser SVM nur möglich, wenn der Standort der SVM nicht berücksichtigt wird. Im Abschnitt **Algorithmus zur SVM-Auswahl** müssen Sie die Option **SVM-Standort** auf **SVM-Standort ignorieren** festlegen. Bei einem beliebigen anderen angegebenen Wert kann der Light Agent keine Verbindung zur SVM herstellen.

   b. Wenn Sie "Integrationsserver verwenden" ausgewählt haben, werden im Fenster des Assistenten die aktuellen Verbindungsparameter der Light Agents mit dem Integrationsserver angezeigt: Adresse und Port für die Verbindung. Bei Bedarf können Sie neue Verbindungsparameter angeben:

      a. Klicken Sie auf die Schaltfläche **Konfigurieren** und geben Sie im neuen Fenster die neuen Verbindungsparameter an:

         - **Adresse**

           IP-Adresse im IPv4-Format oder als vollqualifizierter Domänenname (FQDN) des Geräts mit installiertem Integrationsserver.

           Wenn als Adresse der NetBIOS-Name, "localhost" oder "127.0.0.1" angegeben wird, schlägt die Verbindung zum Integrationsserver mit einem Fehler fehl.

         - **Port**

Port für die Verbindung zum Integrationsserver.

Standardmäßig ist Port 7271 angegeben.

b. Klicken Sie auf **Untersuchen**.

c. Das Web-Plug-in untersucht das vom Integrationsserver empfangene SSL-Zertifikat. Wenn das Zertifikat einen Fehler enthält oder nicht vertrauenswürdig ist, wird im Fenster **Verbindung zum Integrationsserver** eine entsprechende Meldung angezeigt.

Sie können die Informationen über das vom Integrationsserver abgerufene Zertifikat anzeigen, indem Sie auf die Zeile **Abgerufenes Zertifikat anzeigen** klicken. Falls Probleme mit einem SSL-Zertifikat auftreten, empfiehlt es sich, sicherzustellen, dass der von Ihnen verwendete Kanal zur Datenübertragung sicher ist.

Um das empfangene Zertifikat zu speichern und die Verbindung mit dem Integrationsserver fortzusetzen, wählen Sie im Block **Aktion auswählen** die Option **Ignorieren** aus.

d. Geben Sie das Administratorkennwort des Integrationsservers (Kennwort des Kontos `admin`) an und klicken Sie auf die Schaltfläche **Untersuchen**.

Der Assistent für das Erstellen einer Richtlinie stellt eine Verbindung zum Integrationsserver her. Wenn die Verbindung fehlschlägt, wird im Fenster eine Fehlermeldung angezeigt. Wenn die Verbindung hergestellt ist, wird das Fenster **Verbindung zum Integrationsserver** geschlossen und im Fenster des Assistenten für das Erstellen einer Richtlinie im Feld **Verbindung zum Integrationsserver** der Status **Hergestellt** angezeigt.

c. Wenn Sie "Manuell hinzugefügte Liste mit SVM-Adressen verwenden" ausgewählt haben, zeigt das Fenster eine Liste der SVMs an, mit denen Light Agents, die von dieser Richtlinie verwaltet werden, eine Verbindung herstellen können. Um eine SVM zur Liste hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie im angezeigten Fenster die IP-Adresse im IPv4-Format oder den vollqualifizierten Domänennamen (FQDN) der SVM an. Sie können IP-Adressen oder vollqualifizierte Domänennamen von SVMs in einer neuen Zeile eingeben.

Es können nur vollqualifizierte Domänennamen (FQDNs) angeben werden, die jeweils einer einzelnen IP-Adresse entsprechen. Die Verwendung eines vollständig qualifizierten Domänennamens, der mehreren IP-Adressen entspricht, kann zu Fehlern in der App führen.

Sie können in der Liste ausgewählte Adressen löschen, indem Sie auf die Schaltfläche **Löschen** klicken.

Wechseln Sie zum nächsten Schritt des Assistenten.

7. Entscheidung Sie sich über die Verwendung von Kaspersky Security Network. Lesen Sie sich dazu die Erklärung zu Kaspersky Security Network aufmerksam durch und führen Sie dann eine der folgenden Aktionen aus:

- Wenn Sie mit allen Punkten der Erklärung einverstanden sind und Kaspersky Security Network während der Ausführung der App verwenden möchten, wählen Sie die Option **Ich bestätige, dass ich die Bestimmungen und Bedingungen der Erklärung zu Kaspersky Security Network vollständig gelesen habe und sie verstehe und akzeptiere**.

- Wenn Sie der Verwendung von Kaspersky Security Network nicht zustimmen möchten, wählen Sie die Variante **Ich lehne die Erklärung zu Kaspersky Security Network ab** und bestätigen Sie Ihre Entscheidung im folgenden Fenster.

Wenn Sie die Verwendung von Kaspersky Security Network ablehnen, wird die Richtlinienerstellung nicht unterbrochen. Sie können jederzeit die Verwendung von Kaspersky Security Network aktivieren oder deaktivieren, oder den von den verwalteten Geräten verwendeten Modus von Kaspersky Security Network in den Richtlinieneinstellungen ändern.

Wechseln Sie zum nächsten Schritt des Assistenten.

8. Das Fenster mit den Einstellungen der neuen Richtlinie wird geöffnet; die Registerkarte **Allgemein** ist darin ausgewählt. Geben Sie einen Namen der neuen Richtlinie ein.

   Sie können außerdem die folgenden Einstellungen der Richtlinie konfigurieren:

   - Richtlinienstatus:

     - **Aktiv**. Die aktuell auf das Gerät angewendete Richtlinie. Wenn diese Option ausgewählt ist, wird diese Richtlinie bei der nächsten Synchronisierung des Geräts mit dem Administrationsserver auf dem Gerät aktiv. Diese Option ist standardmäßig ausgewählt.

     - **Inaktiv**. Eine Richtlinie, die derzeit nicht auf das Gerät angewendet wird. Wenn diese Option ausgewählt ist, wird die Richtlinie inaktiv, verbleibt jedoch im Ordner **Richtlinien**. Später können Sie die inaktive Richtlinie aktivieren.

   - Vererbung von Richtlinieneinstellungen:

     - **Einstellungen aus übergeordneter Richtlinie erben**. Wenn der Umschalter aktiviert ist, werden die Werte der Richtlinieneinstellung von der Gruppenrichtlinie höherer Ebene geerbt und sind deshalb gesperrt. Der Schalter ist standardmäßig aktiviert.

     - **Vererbung von Einstellungen aus der übergeordneten Richtlinie erzwingen**. Wenn der Umschalter aktiviert ist, können die Werte der untergeordneten Richtlinieneinstellungen nicht geändert werden. Der Schalter ist standardmäßig deaktiviert.

   Allgemeine Informationen zu den Richtlinieneinstellungen finden Sie in der Dokumentation zu Kaspersky Security Center.

9. Wenn Sie andere Richtlinieneinstellungen konfigurieren möchten, wechseln Sie zur Registerkarte **App-Einstellungen** und nehmen Sie die erforderlichen Änderungen vor.

   Die Richtlinieneinstellungen können auch zu einem späteren Zeitpunkt angepasst werden.

10. Klicken Sie auf **Speichern**.

Die erstellte Richtlinie erscheint in der Liste mit Richtlinien.

Allgemeine Informationen über die Verwaltung von Richtlinien finden Sie in der Dokumentation zu Kaspersky Security Center.

Richtlinieneinstellungen in der Web Console ändern

So ändern Sie Richtlinieneinstellungen in der Web Console:

1. Wählen Sie im Hauptfenster von Web Console **Assets (Geräte)** → **Richtlinien und Richtlinienprofile**.

   Die Liste mit Richtlinien wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die die Geräte enthält, auf die die Richtlinie angewendet wird. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

   In der Liste werden die Richtlinien angezeigt, die für die ausgewählte Administrationsgruppe konfiguriert sind.

3. Klicken Sie in der Liste auf den Namen der erforderlichen Richtlinie.

Das Eigenschaftenfenster der Richtlinie wird geöffnet.

4. Ändern Sie die Richtlinieneinstellungen auf der Registerkarte **App-Einstellungen**.

5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die Richtlinie wird mit den aktualisierten Einstellungen gespeichert.

Richtlinieneinstellungen in der Web Console

Die Auswahl von Einstellungen sowie die Standardwerte der Richtlinieneinstellungen sind abhängig von der Lizenz, mit der die App aktiviert wurde. Je nachdem, in welchem Modus die App verwendet wird, werden einige Richtlinieneinstellungen möglicherweise auf die App angewendet oder nicht. Außerdem werden einige Funktionen der App in KESL-Containern nicht unterstützt.

Sie können Richtlinieneinstellungen auf der Registerkarte **App-Einstellungen** im Fenster der Richtlinieneigenschaften konfigurieren.

Richtlinieneinstellungen

Abschnitt	Unterabschnitte
Basisschutz	Schutz vor bedrohlichen Dateien Ausschlüsse aus dem Schutz vor bedrohlichen Dateien Firewall-Verwaltung Schutz vor Web-Bedrohungen Schutz vor Netzwerkbedrohungen
Erweiterter Schutz	Kaspersky Security Network Schutz vor Verschlüsselung Verhaltensanalyse
Detection and Response	Managed Detection and Response Endpoint Detection and Response Optimum Endpoint Detection and Response (KATA)
Sicherheitskontrolle	App-Kontrolle Gerätekontrolle Überwachung der Systemintegrität Web-Kontrolle
Lokale Aufgaben	Aufgabenverwaltung Untersuchung von Wechseldatenträgern
Allgemeine Einstellungen	Proxy-Server-Einstellungen Anwendungseinstellungen Einstellungen der Container-Untersuchung Netzwerkeinstellungen Globale Ausschlüsse Speichereinstellungen
Light Agent-Modus	Einstellungen der SVM-Erkennung

	Einstellung der Verbindung zum Integrationsserver Tag der Verbindung zur SVM Algorithmus der SVM-Auswahl Verbindung absichern

Richtlinien in der Verwaltungskonsole verwalten

In der Kaspersky Security Center Verwaltungskonsole können Sie folgende Aktionen für Richtlinien ausführen:

- Richtlinie erstellen
- Richtlinieneinstellungen ändern

  Wenn das Benutzerkonto, mit dem der Zugriff auf den Administrationsserver erfolgt, nicht zum Bearbeiten von Einstellungen einzelner Funktionsbereiche berechtigt ist, können die Einstellungen dieser Funktionsbereiche nicht bearbeitet werden. Außerdem wird die Konfiguration einiger Einstellungen im KESL-Container nicht unterstützt.

- Richtlinieneinstellungen exportieren und importieren
- Richtlinie löschen
- Status der Richtlinie ändern
- Richtlinienprofile erstellen

Allgemeine Informationen zur Verwendung von Richtlinien finden Sie in der Hilfe zu Kaspersky Security Center.

Richtlinien mithilfe der Verwaltungskonsole erstellen

So erstellen Sie eine Richtlinie in der Verwaltungskonsole:

1. Wählen Sie in der Struktur der Verwaltungskonsole im Ordner **Verwaltete Geräte** die Administrationsgruppe aus, die die Geräte enthält, für welche die Richtlinie angewendet werden soll.

   Auf der Registerkarte **Geräte** des Ordners mit dem Namen der Administrationsgruppe können Sie die Liste der Geräte anzeigen, die zu dieser Administrationsgruppe gehören.

2. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.

3. Klicken Sie auf die Schaltfläche **Neue Richtlinie**, um den Assistenten für das Erstellen einer Richtlinie zu starten.

   Sie können den Assistenten auch über den Eintrag **Erstellen** → **Richtlinie** im Kontextmenü in der Liste der Richtlinien starten.

4. Wählen Sie im ersten Schritt des Assistenten **Kaspersky Endpoint Security 12.1 für Linux** aus der Liste aus.

   Wechseln Sie zum nächsten Schritt des Assistenten.

5. Geben Sie einen Namen der neuen Richtlinie ein.

6. Wenn Sie die Einstellungen aus der Richtlinie einer früheren Programmversion von Kaspersky Endpoint Security in die zu erstellende Richtlinie übertragen möchten, aktivieren Sie das Kontrollkästchen **Richtlinieneinstellungen einer früheren Programmversion verwenden**.

   Wechseln Sie zum nächsten Schritt des Assistenten.

7. Entscheidung Sie sich über die Verwendung von Kaspersky Security Network. Lesen Sie sich dazu die Erklärung zu Kaspersky Security Network aufmerksam durch und führen Sie dann eine der folgenden Aktionen aus:

   - Wenn Sie mit allen Punkten der Erklärung einverstanden sind und Kaspersky Security Network während der Ausführung der App verwenden möchten, wählen Sie die Option **Ich bestätige, dass ich die Bestimmungen und Bedingungen der Erklärung zu Kaspersky Security Network vollständig gelesen habe und sie verstehe und akzeptiere**.

   - Wenn Sie der Verwendung von Kaspersky Security Network nicht zustimmen möchten, wählen Sie die Variante **Ich lehne die Erklärung zu Kaspersky Security Network ab** und bestätigen Sie Ihre Entscheidung im folgenden Fenster.

   Wenn Sie die Verwendung von Kaspersky Security Network ablehnen, wird die Richtlinienerstellung nicht unterbrochen. Sie können jederzeit die Verwendung von Kaspersky Security Network aktivieren oder deaktivieren, oder den von den verwalteten Geräten verwendeten Modus von Kaspersky Security Network in den Richtlinieneinstellungen ändern.

   Wechseln Sie zum nächsten Schritt des Assistenten.

8. Geben Sie an, in welchem Modus Sie Kaspersky Endpoint Security verwenden:

   - **Standard-Modus zum Schutz von Workstations und Servern** – Die App wird zum Schutz von Geräten verwendet, auf denen Linux-Betriebssysteme ausgeführt werden.

   - **Light Agent-Modus zum Schutz virtueller Umgebungen** – Die App wird im Rahmen von Kaspersky Security for Virtualization Light Agent zum Schutz virtueller Maschinen verwendet, auf denen Linux-Gastbetriebssysteme ausgeführt werden.

   Wechseln Sie zum nächsten Schritt des Assistenten.

9. Wenn Sie die App im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, konfigurieren Sie die Einstellungen zur SVM-Ermittlung:

   a. Wählen Sie die Methode aus, die von den Light Agents verwendet werden soll, um für verfügbare SVMs zum Herstellen einer Verbindung zu erkennen:

      - **Integrationsserver verwenden**

        Wenn diese Option ausgewählt ist, stellt der Light Agent eine Verbindung zum Integrationsserver her, um eine Liste der für die Verbindung verfügbaren SVMs und Informationen darüber zu erhalten.

      - **Manuell hinzugefügte Liste mit SVM-Adressen verwenden**

        Wenn diese Option ausgewählt ist, können Sie eine Liste von SVMs angeben, mit denen Light Agents, die durch diese Richtlinie verwaltet werden, eine Verbindung herstellen können. Die Light Agents stellen nur Verbindungen zu den in der Liste angegebenen SVMs her.

Wenn Sie die Option **Manuell hinzugefügte Liste mit SVM-Adressen verwenden** ausgewählt haben und für den Light Agent der erweiterte Algorithmus zur SVM-Auswahl verwendet wird sowie auf der SVM der Modus zum Schutz großer Infrastrukturen aktiviert ist (mehr dazu finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent), dann ist die Verbindung eines Light Agents mit dieser SVM nur möglich, wenn der Standort der SVM nicht berücksichtigt wird. Im Abschnitt **Algorithmus zur SVM-Auswahl** müssen Sie die Option **SVM-Standort** auf **SVM-Standort ignorieren** festlegen. Bei einem beliebigen anderen angegebenen Wert kann der Light Agent keine Verbindung zur SVM herstellen.

b. Wenn Sie "Integrationsserver verwenden" ausgewählt haben, werden im Fenster des Assistenten die aktuellen Verbindungsparameter der Light Agents mit dem Integrationsserver angezeigt: Adresse und Port für die Verbindung. Bei Bedarf können Sie neue Verbindungsparameter angeben:

a. Klicken Sie auf die Schaltfläche **Ändern** und geben Sie im neuen Fenster die neuen Verbindungsparameter an:

- **Adresse**

  IP-Adresse im IPv4-Format oder als vollqualifizierter Domänenname (FQDN) des Geräts mit installiertem Integrationsserver.

  Wenn das Gerät mit installierter Kaspersky Security Center Verwaltungskonsole zu einer Domäne gehört, wird in dem Feld standardmäßig der Domänenname des Geräts angegeben.

  Wenn das Gerät mit installierter Kaspersky Security Center Verwaltungskonsole in keiner Domäne enthalten ist oder der Integrationsserver auf einem anderen Gerät installiert ist, muss das Feld manuell ausgefüllt werden.

  Wenn als Adresse der NetBIOS-Name, "localhost" oder "127.0.0.1" angegeben wird, schlägt die Verbindung zum Integrationsserver mit einem Fehler fehl.

- **Port**

  Port für die Verbindung zum Integrationsserver.

  Standardmäßig ist Port 7271 angegeben.

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

c. Für die Authentifizierung am Integrationsserver wird das Administratorkonto des Integrationsservers verwendet, wenn das Gerät mit installierter Kaspersky Security Center Verwaltungskonsole kein Teil einer Domäne ist oder Ihr Konto kein Mitglied in einer der folgenden Gruppen ist: lokalen Gruppe "KLAdmins", Domänengruppe "KLAdmins" oder lokale Administratorengruppe.

Geben Sie im neuen Fenster das Administratorkennwort des Integrationsservers (Kennwort des Kontos `admin`) an und klicken Sie auf die Schaltfläche **OK**.

d. Das MMC-Plug-in untersucht das vom Integrationsserver empfangene SSL-Zertifikat. Wenn das Zertifikat einen Fehler enthält oder nicht vertrauenswürdig ist, wird das Fenster **Überprüfung des Zertifikats vom Integrationsserver** geöffnet. Über den Link im Fenster können Sie Informationen zum erhaltenen Zertifikat anzeigen.

Falls Probleme mit einem SSL-Zertifikat auftreten, empfiehlt es sich, sicherzustellen, dass der von Ihnen verwendete Kanal zur Datenübertragung sicher ist.

Um die Herstellung der Verbindung zum Integrationsserver fortzusetzen, klicken Sie auf die Schaltfläche **Ignorieren**. Das empfangene Zertifikat wird als vertrauenswürdiges Zertifikat auf dem Gerät mit installierter Kaspersky Security Center Verwaltungskonsole installiert.

c. Wenn Sie "Manuell hinzugefügte Liste mit SVM-Adressen verwenden" ausgewählt haben, zeigt das Fenster eine Liste der SVMs an, mit denen Light Agents, die von dieser Richtlinie verwaltet werden, eine Verbindung herstellen können. Um eine SVM zur Liste hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie im angezeigten Fenster die IP-Adresse im IPv4-Format oder den vollqualifizierten Domänennamen (FQDN) der SVM an. Sie können IP-Adressen oder vollqualifizierte Domänennamen von SVMs in einer neuen Zeile eingeben.

> Es können nur vollqualifizierte Domänennamen (FQDNs) angeben werden, die jeweils einer einzelnen IP-Adresse entsprechen. Die Verwendung eines vollständig qualifizierten Domänennamens, der mehreren IP-Adressen entspricht, kann zu Fehlern in der App führen.

Sie können in der Liste ausgewählte Adressen löschen, indem Sie auf die Schaltfläche **Löschen** klicken.

Wechseln Sie zum nächsten Schritt des Assistenten.

10. Konfigurieren Sie bei Bedarf die allgemeinen Einstellungen für den Schutz vor bedrohlichen Dateien.

    Wechseln Sie zum nächsten Schritt des Assistenten.

11. Ändern Sie bei Bedarf die Standardeinstellungen für den Schutz vor bedrohlichen Dateien.

    Wechseln Sie zum nächsten Schritt des Assistenten.

12. Konfigurieren Sie bei Bedarf die Ausschlüsse aus dem Schutz vor bedrohlichen Dateien.

    Wechseln Sie zum nächsten Schritt des Assistenten.

13. Ändern Sie bei Bedarf die Standardaktionen beim Erkennen einer Bedrohung.

    Wechseln Sie zum nächsten Schritt des Assistenten.

14. Beenden Sie den Assistenten für das Erstellen einer Richtlinie.

Die erstellte Richtlinie wird in der Liste der Richtlinien der Administrationsgruppe auf der Registerkarte **Richtlinien** und im Ordner **Richtlinien** in der Konsolenstruktur angezeigt.

Die Richtlinieneinstellungen können zu einem späteren Zeitpunkt angepasst werden. Allgemeine Informationen über die Verwaltung von Richtlinien finden Sie in der Dokumentation zu Kaspersky Security Center.

Richtlinieneinstellungen in der Kaspersky Security Center Verwaltungskonsole ändern

So ändern Sie Richtlinieneinstellungen in der Verwaltungskonsole:

1. Öffnen Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu der die erforderlichen Geräte gehören.

2. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.

3. Wählen Sie in der Liste der Richtlinien die erforderliche Richtlinie aus und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>** mit einem Doppelklick.

Sie können das Fenster mit den Richtlinieneigenschaften auch über den Eintrag **Eigenschaften** im Kontextmenü der Richtlinie oder durch Klicken auf den Link **Richtlinieneinstellungen konfigurieren** rechts neben der Liste der Richtlinien im Block mit den Richtlinieneinstellungen öffnen.

4. Passen Sie die Richtlinieneinstellungen an.

5. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf **OK**, um die Änderungen zu speichern.

Richtlinieneinstellungen in der Verwaltungskonsole

Die Auswahl von Einstellungen sowie die Standardwerte der Richtlinieneinstellungen sind abhängig von der Lizenz, mit der die App aktiviert wurde. Je nachdem, in welchem Modus die App verwendet wird, werden einige Richtlinieneinstellungen möglicherweise auf die App angewendet oder nicht. Außerdem werden einige Funktionen der App in KESL-Containern nicht unterstützt.

Sie können Richtlinieneinstellungen in Abschnitten und Unterabschnitten im Fenster der Richtlinieneigenschaften konfigurieren. Informationen über die Konfiguration der allgemeinen Richtlinien- und Ereigniseinstellungen finden Sie in der Dokumentation zu Kaspersky Security Center.

Richtlinieneinstellungen

Abschnitt	Unterabschnitte
Basisschutz	Schutz vor bedrohlichen Dateien Ausschlüsse aus dem Schutz vor bedrohlichen Dateien Firewall-Verwaltung Schutz vor Web-Bedrohungen Schutz vor Netzwerkbedrohungen
Erweiterter Schutz	Kaspersky Security Network Schutz vor Verschlüsselung Verhaltensanalyse
Detection and Response	Managed Detection and Response Endpoint Detection and Response (KATA)
Sicherheitskontrolle	App-Kontrolle Gerätekontrolle Überwachung der Systemintegrität Web-Kontrolle
Lokale Aufgaben	Aufgabenverwaltung Untersuchung von Wechseldatenträgern
Allgemeine Einstellungen	Proxy-Server-Einstellungen Anwendungseinstellungen Einstellungen der Container-Untersuchung Netzwerkeinstellungen Globale Ausschlüsse Prozess-Speicher ausschließen

	Speichereinstellungen
Light Agent-Modus	Verbindung zum Integrationsserver Einstellungen der SVM-Erkennung Tag der Verbindung zur SVM Algorithmus der SVM-Auswahl Verbindung absichern

Aufgabenverwaltung in Web Console

Sie können die folgenden Aktionen für Aufgaben für Kaspersky Endpoint Security in der Web Console ausführen:

- Neue Aufgaben erstellen.
- Aufgabeneinstellungen ändern.

  Wenn das Benutzerkonto, mit dem der Zugriff auf den Administrationsserver erfolgt, nicht zum Bearbeiten von Einstellungen einzelner Funktionsbereiche berechtigt ist, können die Einstellungen dieser Funktionsbereiche nicht bearbeitet werden. Außerdem wird die Konfiguration einiger Einstellungen im KESL-Container nicht unterstützt.

- Aufgaben starten, beenden, anhalten und fortsetzen.

  Die *Update-Aufgabe* kann nicht angehalten oder fortgesetzt werden; sie kann nur gestartet und beendet werden.

- Aufgaben exportieren und importieren.
- Aufgaben löschen.

In der Liste der Aufgaben können Sie die Ausführung der Aufgabe überwachen, darunter den Aufgabenstatus und die Statistik zur Aufgabenausführung auf den Geräten. Sie können auch eine Auswahl von Ereignissen erstellen, um den Abschluss von Aufgaben zu überwachen (**Überwachung und Berichterstattung** → **Ereignisauswahlen**). Nähere Informationen zur Ereignisauswahl finden Sie in der Dokumentation zu Kaspersky Security Center.

Die Ergebnisse der Aufgabenausführung werden auch lokal auf dem Gerät und in den Berichten von Kaspersky Security Center gespeichert.

Allgemeine Informationen zur Verwendung von Aufgaben finden Sie in der Hilfe zu Kaspersky Security Center.

Wenn das Gerät durch eine Richtlinie verwaltet wird, können in Kaspersky Security Center erstellte Aufgaben möglicherweise nicht über die Befehlszeile oder die lokale Benutzeroberfläche auf dem Gerät angezeigt und verwaltet werden.

Aufgabenerstellung in der Web Console

So erstellen Sie eine Aufgabe in der Web Console:

1. Wählen Sie im Hauptfenster der Web Console die Option **Assets (Geräte)** → **Aufgaben**.

   Die Liste mit Aufgaben wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Gehen Sie im ersten Schritt des Assistenten folgendermaßen vor:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** den Eintrag **Kaspersky Endpoint Security 12.1 für Linux**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Aufgabentyp aus, den Sie erstellen möchten.

   c. Geben Sie im Feld **Aufgabenname** den Namen der neuen Aufgabe ein.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** eine Methode zur Definition des Gültigkeitsbereichs der Aufgabe aus. Der Gültigkeitsbereich einer Aufgabe sind die Geräte, auf denen die Aufgabe ausgeführt wird:

      - Wählen Sie die Option **Aufgabe einer Administrationsgruppe zuweisen**, wenn die Aufgabe auf allen Geräten ausgeführt werden soll, die zu einer bestimmten Administrationsgruppe gehören.

      - Wählen Sie die Option **Geräteadressen manuell angeben oder aus Liste importieren**, wenn die Aufgabe auf bestimmten Geräten ausgeführt werden soll.

      - Wählen Sie die Option **Aufgabe einer Geräteauswahl zuweisen**, wenn die Aufgabe auf Geräten ausgeführt werden soll, die zu einer nach vordefinierten Kriterien getroffenen Geräteauswahl gehören. Informationen zum Erstellen einer Geräteauswahl finden Sie in der Hilfe zu Kaspersky Security Center.

   Wechseln Sie zum nächsten Schritt des Assistenten.

4. Führen Sie abhängig von der ausgewählten Methode zur Definition des Gültigkeitsbereichs der Aufgabe eine der folgenden Aktionen aus:

   - Aktivieren Sie in der Baumstruktur der Administrationsgruppen die Kontrollkästchen neben den erforderlichen Administrationsgruppen.

   - Aktivieren Sie in der Geräteliste die Kontrollkästchen neben den erforderlichen Geräten. Wenn die erforderlichen Geräte nicht in der Liste enthalten sind, können Sie sie auf folgende Weise hinzufügen:

      - Über die Schaltfläche **Geräte hinzufügen**. Sie können Geräte nach Namen oder IP-Adresse hinzufügen, Geräte aus einem bestimmten IP-Bereich hinzufügen oder Geräte aus der Liste der Geräte auswählen, die der Administrationsserver bei der Abfrage des lokalen Unternehmensnetzwerks erkannt hat.

      - Über die Schaltfläche **Geräte aus Datei importieren**. Zum Importieren wird eine TXT-Datei mit einer Liste von Geräteadressen verwendet, wobei jede Adresse in einer separaten Zeile stehen muss.

   - Wählen Sie in der Liste den Namen der Auswahl aus, in der die erforderlichen Geräte enthalten sind.

   Wechseln Sie zum nächsten Schritt des Assistenten.

5. Um die Aufgabeneinstellungen direkt nach der Erstellung zu konfigurieren, aktivieren Sie im letzten Schritt des Assistenten das Kontrollkästchen **Fenster mit den Aufgabeneigenschaften nach der Erstellung öffnen**. Die Aufgabe wird mit Standardeinstellungen erstellt.

6. Beenden Sie den Assistenten.

Eine neue Aufgabe wird in der Liste mit Aufgaben angezeigt.

Aufgabeneinstellungen in der Web Console ändern

So ändern Sie Aufgabeneinstellungen in der Web Console:

1. Wählen Sie im Hauptfenster der Web Console die Option **Assets (Geräte)** → **Aufgaben**.

   Die Liste mit Aufgaben wird geöffnet.

2. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf allen Geräten einer bestimmten Administrationsgruppe ausgeführt wird, klicken Sie auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

     In der Liste werden nur die Aufgaben angezeigt, die für die ausgewählte Administrationsgruppe konfiguriert sind.

   - Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf einem oder mehreren Geräten ausgeführt wird (Aufgaben für eine Gerätegruppe), klicken Sie auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster den oberen Knoten mit dem Namen des Administrationsservers.

     In der Liste werden alle auf dem Administrationsserver erstellten Aufgaben angezeigt.

3. Wählen Sie in der Aufgabenliste die erforderliche Aufgabe aus und öffnen Sie über den Link im Aufgabennamen das Fenster mit den Aufgabeneigenschaften.

4. Konfigurieren Sie die Aufgabeneinstellungen:

   - Auf der Registerkarte **Allgemein** können Sie den Namen der Aufgabe ändern.

   - Auf der Registerkarte **App-Einstellungen** können Sie die spezifischen Aufgabeneinstellungen konfigurieren. Die Verfügbarkeit konfigurierbarer Parameter hängt vom Aufgabentyp ab.

   - Auf der Registerkarte **Zeitplan** können Sie den Zeitplan für den Aufgabenstart und zusätzliche Einstellungen zum Starten und Beenden der Aufgabe konfigurieren.

   Die Registerkarten **Allgemein**, **Ergebnisse**, **Einstellungen**, **Zeitplan** und **Revisionsverlauf** des Eigenschaftenfensters der Aufgabe sind für Kaspersky Security Center vordefiniert. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security Center.

5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Aufgaben in der Web Console starten, beenden, anhalten und fortsetzen

So können Sie eine Aufgabe in der Web Console starten, beenden, anhalten oder fortsetzen:

1. Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console **Assets (Geräte)** → **Aufgaben**.

   Die Liste mit Aufgaben wird geöffnet.

2. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie eine Aufgabe starten oder beenden möchten, die auf allen Geräten einer bestimmten Administrationsgruppe ausgeführt wird, klicken Sie auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

     In der Liste werden nur die Aufgaben angezeigt, die für die ausgewählte Administrationsgruppe erstellt wurden.

   - Wenn Sie eine Aufgabe starten oder beenden möchten, die auf einem oder mehreren Geräten ausgeführt wird (Aufgabe für eine Gerätegruppe), klicken Sie auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster den oberen Knoten mit dem Namen des Administrationsservers.

     In der Liste werden alle auf dem Administrationsserver erstellten Aufgaben angezeigt.

3. Aktivieren Sie in der Liste der Aufgaben das Kontrollkästchen neben dem Namen der erforderlichen Aufgabe und klicken Sie auf die Schaltfläche für die erforderliche Aktion über der Liste der Aufgaben.

Aufgaben in der Verwaltungskonsole verwalten

Sie können die folgenden Aktionen für Aufgaben für Kaspersky Endpoint Security in der Verwaltungskonsole ausführen:

- Neue Aufgaben erstellen.
- Aufgabeneinstellungen ändern.

  > Wenn das Benutzerkonto, mit dem der Zugriff auf den Administrationsserver erfolgt, nicht zum Bearbeiten von Einstellungen einzelner Funktionsbereiche berechtigt ist, können die Einstellungen dieser Funktionsbereiche nicht bearbeitet werden. Außerdem wird die Konfiguration einiger Einstellungen im KESL-Container nicht unterstützt.

- Aufgaben starten, beenden, anhalten und fortsetzen.

  > Die *Update-Aufgabe* kann nicht angehalten oder fortgesetzt werden; sie kann nur gestartet und beendet werden.

- Aufgaben exportieren und importieren.
- Aufgaben löschen.

In der Liste der Aufgaben können Sie die Ausführung der Aufgabe überwachen, darunter den Aufgabenstatus und die Statistik zur Aufgabenausführung auf den Geräten.

Informationen über den Fortschritt und die Ergebnisse der Aufgabenausführung können Sie in der Liste der Ereignisse anzeigen, die Kaspersky Endpoint Security an den Kaspersky Security Center Administrationsserver sendet (auf der Registerkarte **Ereignisse** im Arbeitsbereich des Knotens **Administrationsserver <Servername>**). Sie können auch eine Auswahl von Ereignissen erstellen, um die Ausführung von Aufgaben zu überwachen. Nähere Informationen zur Ereignisauswahl finden Sie in der Dokumentation zu Kaspersky Security Center.

Die Ergebnisse der Aufgabenausführung werden auch lokal auf dem Gerät und in den Berichten von Kaspersky Security Center gespeichert.

Allgemeine Informationen zur Verwendung von Aufgaben finden Sie in der Hilfe zu Kaspersky Security Center.

Wenn das Gerät durch eine Richtlinie verwaltet wird, können in Kaspersky Security Center erstellte Aufgaben möglicherweise nicht über die Befehlszeile oder die lokale Benutzeroberfläche auf dem Gerät angezeigt und verwaltet werden.

Aufgaben in der Verwaltungskonsole erstellen

So erstellen Sie eine Aufgabe in der Verwaltungskonsole:

1. Führen Sie in der Verwaltungskonsole eine der folgenden Aktionen aus:

   - Wenn Sie eine Aufgabe erstellen möchten, die auf Geräten ausgeführt wird, die zur ausgewählten Administrationsgruppe gehören, wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** diese Administrationsgruppe aus, wählen Sie dann im Arbeitsbereich die Registerkarte **Aufgaben** aus und klicken Sie auf die Schaltfläche **Neue Aufgabe**.

     Der Assistent für das Erstellen einer Aufgabe für Geräte der ausgewählten Administrationsgruppe wird gestartet.

   - Wenn Sie eine Aufgabe erstellen möchten, die auf einem oder mehreren Geräten ausgeführt wird (Aufgabe für eine Gerätegruppe), wählen Sie den Ordner **Aufgaben** in der Konsolenstruktur aus und klicken Sie im Arbeitsbereich auf die Schaltfläche **Neue Aufgabe**.

     Der Assistent für das Erstellen einer Aufgabe für eine Gerätegruppe wird gestartet.

2. Wählen Sie im ersten Schritt des Assistenten **Kaspersky Endpoint Security 12.1 für Linux** und den Aufgabentyp aus.

   Wechseln Sie zum nächsten Schritt des Assistenten.

3. Wenn Sie eine Aufgabe für eine Gerätegruppe erstellen, werden Sie vom Assistenten aufgefordert, den Gültigkeitsbereich der Aufgabe zu definieren. Der Gültigkeitsbereich einer Aufgabe sind die Geräte, auf denen die Aufgabe ausgeführt wird.

   a. Geben Sie die Methode zur Definition des Gültigkeitsbereichs der Aufgabe an: Wählen Sie Geräte aus der Liste der vom Administrationsserver erkannten Geräte aus, geben Sie die Geräteadressen manuell ein, importieren Sie eine Geräteliste aus einer Datei oder geben Sie eine zuvor konfigurierte Geräteauswahl an (weitere Einzelheiten finden Sie in der Hilfe zu Kaspersky Security Center).

   b. Führen Sie abhängig von der Methode, die Sie zum Definieren des Gültigkeitsbereichs im angezeigten Fenster angegeben haben, eine der folgenden Aktionen aus:

      - Geben Sie in der Liste der erkannten Geräte die Geräte an, auf denen die Aufgabe ausgeführt werden soll. Aktivieren Sie dazu das Kontrollkästchen in der Liste links neben dem Gerätenamen.

      - Klicken Sie auf die Schaltfläche **Hinzufügen** oder **IP-Bereich hinzufügen** und geben Sie die Geräteadressen manuell an.

      - Klicken Sie auf die Schaltfläche **Importieren** und wählen Sie im angezeigten Fenster eine TXT-Datei mit einer Liste von Geräteadressen aus.

      - Klicken Sie auf die Schaltfläche **Durchsuchen** und geben Sie im angezeigten Fenster den Namen der Auswahl an, die die Geräte enthält, auf denen die Aufgabe ausgeführt werden soll.

Wechseln Sie zum nächsten Schritt des Assistenten.

4. Konfigurieren Sie die verfügbaren Aufgabeneinstellungen, indem Sie den Anweisungen des Assistenten folgen.

5. Geben Sie einen Namen für die neue Aufgabe ein und fahren Sie mit dem nächsten Schritt des Assistenten fort.

6. Wenn Sie möchten, dass die Aufgabe sofort nach Abschluss des Assistenten gestartet wird, aktivieren Sie im letzten Schritt das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten** starten.

7. Beenden Sie den Assistenten.

   Eine neue Aufgabe wird in der Liste mit Aufgaben angezeigt.

Aufgabeneinstellungen in der Verwaltungskonsole ändern

So ändern Sie Aufgabeneinstellungen in der Verwaltungskonsole:

1. Führen Sie in der Verwaltungskonsole eine der folgenden Aktionen aus:

   - Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf Geräten ausgeführt wird, die zu einer bestimmten Administrationsgruppe gehören, wählen Sie diese Administrationsgruppe in der Konsolenstruktur aus und wählen Sie dann im Arbeitsbereich die Registerkarte **Aufgaben** aus.

   - Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf einem oder mehreren Geräten ausgeführt wird (Aufgaben für eine Gerätegruppe), wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.

2. Wählen Sie in der Aufgabenliste die erforderliche Aufgabe aus und öffnen Sie das Fenster **Eigenschaften: <Aufgabenname>** mit einem Doppelklick.

   Sie können das Eigenschaftenfenster der Aufgabe auch über den Eintrag **Eigenschaften** im Kontextmenü der Aufgabe öffnen.

3. Ändern Sie die Einstellungen der Aufgabe. Die Verfügbarkeit konfigurierbarer Parameter hängt vom Aufgabentyp ab.

   Die Registerkarten **Allgemein**, **Benachrichtigungen**, **Zeitplan** und **Revisionsverlauf** des Eigenschaftenfensters der Aufgabe sind für Kaspersky Security Center vordefiniert. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security Center.

4. Klicken Sie im Fenster **Eigenschaften: <Aufgabenname>** auf die Schaltfläche **Übernehmen** oder die Schaltfläche **OK**, um die Änderungen zu speichern.

Aufgaben in der Verwaltungskonsole starten, beenden, anhalten und fortsetzen

So können Sie eine Aufgabe in der Verwaltungskonsole starten, beenden, anhalten oder fortsetzen:

1. Führen Sie in der Verwaltungskonsole eine der folgenden Aktionen aus:

   - Wenn Sie eine Aufgabe starten oder beenden möchten, die auf Geräten ausgeführt wird, die zu einer bestimmten Administrationsgruppe gehören, wählen Sie diese Administrationsgruppe in der

Konsolenstruktur aus und wählen Sie dann im Arbeitsbereich die Registerkarte **Aufgaben** aus.

Die Liste mit den für die ausgewählte Administrationsgruppe erstellten Aufgaben wird geöffnet.

- Wenn Sie eine Aufgabe starten oder beenden möchten, die auf einem oder mehreren Geräten ausgeführt wird (Aufgaben für eine Gerätegruppe), wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.

  Die Liste mit allen auf dem Administrationsserver erstellten Aufgaben wird geöffnet.

2. Wählen Sie in der Aufgabenliste die erforderliche Aufgabe aus, öffnen Sie das Kontextmenü der Aufgabe und wählen Sie die Aktion aus, die Sie ausführen möchten.

App über die Befehlszeile verwalten

Über die Befehlszeile können Sie Kaspersky Endpoint Security auf dem Gerät installieren und deinstallieren, starten und beenden sowie die Ausführung der App lokal verwalten.

Die Ausführung der Funktionskomponenten der App wird durch *lokale Aufgaben von Kaspersky Endpoint Security* sichergestellt, die im Betriebssystem ausgeführt werden Sie können die Funktionskomponenten der App auf dem Gerät aktivieren oder deaktivieren, indem Sie Aufgaben von Kaspersky Endpoint Security über die Befehlszeile starten und beenden. Einmalige Untersuchungen des Geräts werden auch durch Starten von Aufgaben für Kaspersky Endpoint Security durchgeführt. Sie können die Ausführungseinstellungen der Funktionskomponenten auf dem Gerät und die Einstellungen für die Untersuchung des Geräts festlegen, indem Sie die *Aufgabeneinstellungen* für Kaspersky Endpoint Security konfigurieren.

Zusätzlich zu den Aufgabeneinstellungen stehen die folgenden Einstellungen zur Konfiguration der App-Ausführung zur Verfügung:

- Allgemeine Einstellungen der Container-Untersuchung.
- Einstellungen der Untersuchung geschützter Verbindungen.
- Allgemeine App-Einstellungen, die die Ausführung der App als Ganzes und die Ausführung einzelner Funktionen bestimmen.

Kaspersky Endpoint Security wird über die Befehlszeile mithilfe der *Verwaltungsbefehle für Kaspersky Endpoint Security* verwaltet.

Aktivieren der automatischen Vervollständigung des kesl-control-Befehls (Bash-Vervollständigung)

Für die Bash-Shell kann die automatische Vervollständigung des Befehls kesl-control aktiviert werden.

Um die automatische Vervollständigung des Befehls kesl-control in der aktuellen Bash-Shell-Sitzung zu aktivieren, führen Sie den folgenden Befehl aus:

```
source /opt/kaspersky/kesl/shared/bash_completion.sh
```

Um die automatische Vervollständigung für alle neuen Bash-Shell-Sitzungen zu aktivieren, führen Sie den folgenden Befehl aus:

```
echo "source /opt/kaspersky/kesl/shared/bash_completion.sh" >> ~/.bashrc
```

Aufgaben über die Befehlszeile verwalten

Zur Verwaltung von Kaspersky Endpoint Security über die Befehlszeile sind die folgenden App-Aufgaben vorgesehen:

- *Schutz vor bedrohlichen Dateien*. Mit dieser Aufgabe können Sie den Echtzeitschutz vor bedrohlichen Dateien aktivieren und deaktivieren und Einstellungen für die Komponente "Schutz vor bedrohlichen Dateien" definieren. Die Aufgabe startet automatisch, wenn die App gestartet wird.

- *Schadsoftware-Untersuchung*. Mit dieser Aufgabe können Sie Objekte des Dateisystems auf Befehl auf Schadsoftware untersuchen und Einstellungen für die Untersuchung definieren. Mit dieser Aufgabe können Sie eine vollständige oder benutzerdefinierte Untersuchung des Geräts durchführen.

- *Untersuchung wichtiger Bereiche*. Mit dieser Aufgabe können Sie kritische Bereiche des Betriebssystems auf Befehl untersuchen und Einstellungen für die Untersuchung definieren.

- *Benutzerdefinierte Untersuchung von Dateien*. Mit dieser Aufgabe können Sie Einstellungen konfigurieren und speichern, die während der Untersuchung bestimmter Dateien und Verzeichnisse mit dem Befehl `kesl-control --scan-file` verwendet werden. Als Ergebnis der Ausführung des Befehls erstellt und startet die App eine temporäre Aufgabe zur Untersuchung von Dateien.

- *Untersuchung von Containern*. Mit dieser Aufgabe können Sie Container und Images auf Befehl untersuchen und Einstellungen für die Untersuchung definieren.

- *Benutzerdefinierte Untersuchung von Containern*. Mit dieser Aufgabe können Sie Einstellungen konfigurieren und speichern, die während der Untersuchung bestimmter Container und Images mit dem Befehl `kesl-control [-T] --scan-container` verwendet werden. Als Ergebnis der Ausführung des Befehls erstellt und startet die App eine temporäre Aufgabe zur Untersuchung von Containern.

- *Untersuchung von Wechseldatenträgern*. Mit dieser Aufgabe können Sie die Verbindung von Wechseldatenträgern mit dem Gerät in Echtzeit überwachen und die Einstellungen für die Untersuchung von Wechseldatenträgern und ihren Bootsektoren auf Schadsoftware definieren.

- *Schutz vor Web-Bedrohungen*. Mit dieser Aufgabe können Sie den Schutz vor Web-Bedrohungen aktivieren und deaktivieren und Einstellungen für die Ausführung der Komponente "Schutz vor Web-Bedrohungen" definieren.

- *Schutz vor Netzwerkbedrohungen*. Mit dieser Aufgabe können Sie den Schutz vor Netzwerkbedrohungen aktivieren und deaktivieren und Einstellungen für die Ausführung der Komponente "Schutz vor Netzwerkbedrohungen" definieren.

- *Schutz vor Verschlüsselung*. Mit dieser Aufgabe können Sie den Schutz von Dateien vor bösartiger Remote-Verschlüsselung aktivieren und deaktivieren und Einstellungen für die Komponente "Schutz vor Verschlüsselung" definieren.

- *Firewall-Verwaltung*. Mit dieser Aufgabe können Sie die Firewall-Verwaltung aktivieren und deaktivieren und Einstellungen für die Überwachung von Netzwerkverbindungen auf dem Gerät definieren.

- *App-Kontrolle*. Mit dieser Aufgabe können Sie die App-Kontrolle aktivieren und deaktivieren und Einstellungen für die Komponente "App-Kontrolle" definieren.

- *Inventarisierung*. Mit dieser Aufgabe können Sie Informationen über alle App -Dateien abrufen, die auf dem Gerät gespeichert sind.

- *Gerätekontrolle*. Mit dieser Aufgabe können Sie die Gerätekontrolle aktivieren und deaktivieren und Einstellungen für die Komponente "Gerätekontrolle" definieren. Die Aufgabe startet automatisch, wenn Kaspersky Endpoint Security gestartet wird.

- *Web-Kontrolle*. Mit dieser Aufgabe können Sie die Web-Kontrolle aktivieren und deaktivieren und Einstellungen für die Komponente "Web-Kontrolle" definieren.

- *Verhaltensanalyse*. Mit dieser Aufgabe können Sie schädliche Aktivitäten von Apps im Betriebssystem überwachen. Die Aufgabe startet automatisch, wenn Kaspersky Endpoint Security gestartet wird.

- *Überwachung der System-Integrität*. Mit dieser Aufgabe können Sie in Echtzeit Aktionen überwachen, die mit Objekten aus dem Überwachungsbereich ausgeführt werden, der in den Einstellungen der Komponente "Überwachung der Systemintegrität" angegeben ist.

- *Überwachung der System-Integrität*. Mit dieser Aufgabe können Sie Dateien und Verzeichnisse, die Sie in den Überwachungsbereich aufgenommen haben, auf Änderungen überprüfen, indem Sie den aktuellen Status des überwachten Objekts mit einem zuvor erfassten Status vergleichen.

- *Backup-Verwaltung*. Mit dieser Aufgabe können Sie Backup-Kopien von Dateien im Backup auf dem Gerät speichern. Die Aufgabe startet automatisch beim Start der App und befindet sich dauerhaft im Arbeitsspeicher des Geräts. Die Aufgabe kann nicht gestartet, beendet oder gelöscht werden.

- *Lizenzverwaltung*. Mit dieser Aufgabe können Sie eine auf dem Gerät installierte App aktivieren. Die Aufgabe startet automatisch beim Start der App und befindet sich dauerhaft im Arbeitsspeicher des Geräts. Die Aufgabe hat keine Einstellungen; Lizenzschlüssel werden über spezielle Verwaltungsbefehle verwaltet. Die Aufgabe kann nicht gestartet, beendet oder gelöscht werden.

- *Update*. Mit dieser Aufgabe können Sie die Aktualisierung der Datenbanken und Module der App nach Zeitplan oder bei Bedarf ausführen und Update-Einstellungen konfigurieren.

- *Rollback des Datenbanken-Updates*. Mit dieser Aufgabe können Sie ein Rollback des letzten Updates der Datenbanken und Module der App durchführen.

- *Integration mit Kaspersky Endpoint Detection and Response (KATA)*. Mit dieser Aufgabe können Sie die Integration mit Kaspersky Endpoint Detection and Response (KATA) aktivieren und deaktivieren und Einstellungen für die Integration definieren.

Jede App-Aufgabe hat einen Namen, der in der Befehlszeile verwendet wird, eine ID und einen Typ (siehe Tabelle unten).

IDs sind für alle Aufgaben eindeutig, auch für Remote-Aufgaben. Die App verwendet die IDs gelöschter Aufgaben nicht noch einmal. Die Nummer der ID einer neuen Aufgabe folgt auf die Nummer der ID der zuletzt erstellten Aufgabe.

Bei Aufgabennamen wird die Groß-/Kleinschreibung nicht beachtet.

Während der App-Installation werden *vordefinierte Aufgaben* erstellt. Diese Aufgaben können nicht gelöscht werden. Für jede vordefinierte Aufgabe sind ein Name und eine ID reserviert.

Aufgaben, die Sie während der Verwendung der App erstellen, werden als *Benutzeraufgaben* bezeichnet. Die Namen dieser Aufgaben geben Sie beim Erstellen einer Aufgabe an. Die App definiert und weist einer Aufgabe Benutzeraufgaben-IDs zu, wenn diese erstellt wird. Die IDs für Benutzeraufgaben beginnen bei 100.

Während der Ausführung der App erstellt diese *temporäre Aufgaben zur Untersuchung*. Die Namen und IDs temporärer Aufgaben werden von der App festgelegt. Temporäre Aufgaben werden nach Abschluss automatisch gelöscht.

Aufgabe	Aufgabenname in der Befehlszeile	Aufgaben-ID	Aufgabentyp
Schutz vor bedrohlichen Dateien	File_Threat_Protection	1	OAS
Schadsoftware-Untersuchung	Scan_My_Computer	2	ODS
Schadsoftware-Untersuchung (benutzerdefiniert)	Benutzereingabe	ab 100	ODS
Benutzerdefinierte Untersuchung von Dateien	Scan_File	3	ODS
Untersuchung wichtiger Bereiche	Critical_Areas_Scan	4	ODS
Untersuchung von Containern	Container_Scan	18	ContainerScan
Untersuchung von Containern (benutzerdefiniert)	Benutzereingabe	ab 100	ContainerScan
Benutzerdefinierte Untersuchung von Containern	Custom_Container_Scan	19	ContainerScan
Untersuchung von Wechseldatenträgern	Removable_Drives_Scan	16	RDS
Schutz vor Web-Bedrohungen	Web_Threat_Protection	14	WTP
Schutz vor Netzwerkbedrohungen	Network_Threat_Protection	17	NTP
Schutz vor Verschlüsselung	Anti_Cryptor	13	AntiCryptor
Firewall-Verwaltung	Firewall_Management	12	Firewall
App-Kontrolle	Application_Control	21	AppControl
Inventarisierung	Inventory_Scan	22	InventoryScan
Inventarisierung (benutzerdefiniert)	Benutzereingabe	ab 100	InventoryScan
Gerätekontrolle	Device_Control	15	DeviceControl
Verhaltensanalyse	Behavior_Detection	20	BehaviorDetection
Überwachung der Systemintegrität	System_Integrity_Monitoring	11	OAFIM
Überwachung der Systemintegrität (benutzerdefiniert)	Benutzereingabe	ab 100	ODFIM
Backup-Verwaltung	Backup	10	Backup
Update	Update	6	Update
Update (benutzerdefiniert)	Benutzereingabe	ab 100	Update
Rollback des Datenbanken-Updates	Rollback	7	Rollback
Rollback des Datenbanken-Updates (benutzerdefiniert)	Benutzereingabe	ab 100	Rollback
Lizenzverwaltung	License	9	License
Integration mit Kaspersky Managed Detection and Response (KATA)	KATAEDR	24	KATAEDR
Web-Kontrolle	Web_Control	26	WebControl

Sie können mit Aufgaben folgende Aktionen ausführen:

- Alle vordefinierten Aufgaben und Benutzeraufgaben starten und beenden, mit Ausnahme der Aufgaben vom Typ *Backup* und *License*.
- Aufgaben vom Typ *ODS*, *ODFIM* und *InventoryScan* anhalten und fortsetzen.
- Benutzeraufgaben erstellen und löschen. Abhängig vom Nutzungsmodus der App können Sie Aufgaben der folgenden Typen erstellen:
  - Im Standard-Modus: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* und *InventoryScan*.
  - Im Light Agent-Modus zum Schutz virtueller Umgebungen: *ODS*, *ODFIM*, *ContainerScan* und *InventoryScan*.
- Die Einstellungen aller Benutzeraufgaben und aller vordefinierten Aufgaben ändern, mit Ausnahme der Aufgaben vom Typ *Rollback* und *License*.

  Wenn die App im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, können die Einstellungen der vordefinierten Aufgabe *Update* ebenfalls nicht geändert werden.
- Den Zeitplan für den Aufgabenstart konfigurieren.

Aufgabenliste über die Befehlszeile anzeigen

Um eine Liste mit den Aufgaben der App anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-task-list [--json]
```

Wobei gilt:

`--json` – Ausgabeformat der Liste mit Aufgaben der App Wenn Sie kein Format angeben, erfolgt die Ausgabe im INI-Format.

Zeigt eine Liste mit den Aufgaben von Kaspersky Endpoint Security an.

Für jede Aufgabe werden folgende Informationen angezeigt:

- `Name` – Aufgabenname.
- `ID` – Aufgaben-ID.
- `Type` – Aufgabentyp.
- `State` – Aktueller Status der Aufgabe.

Wenn eine Richtlinie von Kaspersky Security Center den Benutzern das lokale Anzeigen und Bearbeiten von Aufgaben verbietet, werden nur Informationen zu den Aufgaben *Scan_File*, *Backup*, *License*, *File_Threat_Protection*, *System_Integrity_Monitoring* und *Anti_Cryptor* angezeigt. Informationen über andere Aufgaben stehen nicht zur Verfügung.

Aufgabenstatus über die Befehlszeile anzeigen

Führen Sie folgenden Befehl aus, um einen Aufgabenstatus anzuzeigen:

```
kesl-control --get-task-state <ID/Name der Aufgabe> [--json]
```

Wobei gilt:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--json` – Gibt die Einstellungen im JSON-Format aus.

Für die Aufgaben der App sind folgende grundlegende Statusvarianten vorgesehen:

- `Started` – Aufgabe wird ausgeführt
- `Starting` – Aufgabe wird gestartet
- `Stopped` – Aufgabe wurde gestoppt
- `Stopping` – Aufgabe wird gestoppt

Die Aufgaben vom Typ *ODS*, *ODFIM* und *InventoryScan* können außerdem die folgenden Statusvarianten aufweisen:

- `Pausing` – Aufgabe wird angehalten
- `Suspended` – Aufgabe wurde angehalten
- `Resuming` – Aufgabe wird fortgesetzt

Aufgabe über die Befehlszeile erstellen

Wenn die App im Standard-Modus verwendet wird, können Sie Aufgaben der folgenden Typen erstellen: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* und *InventoryScan*.

Wenn die App im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, können Sie Aufgaben der folgenden Typen erstellen: *ODS*, *ODFIM*, *ContainerScan* und *InventoryScan*.

Sie können Aufgaben mit Standardeinstellungen oder mit Einstellungen erstellen, die in einer Konfigurationsdatei angegeben sind.

Um eine Aufgabe mit Standardeinstellungen zu erstellen, führen Sie den folgenden Befehl aus:

```
kesl-control -create-task <Aufgabenname> --type <Aufgabentyp>
```

Wobei gilt:

- `< Aufgabenname >` – Name, den Sie für eine neue Aufgabe vergeben.
- `< Aufgabentyp >` – Bezeichnung des Typs der zu erstellenden Aufgabe.

Um eine Aufgabe mit den Einstellungen zu erstellen, die in einer Konfigurationsdatei angegeben sind, führen Sie den folgenden Befehl aus:

```
kesl-control --create-task < Aufgabenname > --type < Aufgabentyp > --file < Pfad der
Konfigurationsdatei > [--json]
```

Wobei gilt:

- `< Aufgabenname >` – Name, den Sie für eine neue Aufgabe vergeben.
- `< Aufgabentyp >` – Bezeichnung des Typs der zu erstellenden Aufgabe.
- `< Dateipfad >` – Vollständiger Pfad der Konfigurationsdatei, deren Einstellungen beim Erstellen der Aufgabe verwendet werden.
- `--json` – Importiert die Einstellungen aus einer Konfigurationsdatei im JSON-Format. Wenn Sie den Schalter `--json` nicht angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Aufgabe über die Befehlszeile starten, beenden, anhalten und fortsetzen

Sie können vordefinierte Aufgaben und Benutzeraufgaben starten und beenden, mit Ausnahme von Aufgaben vom Typ *Backup* und *License*.

Sie können Aufgaben vom Typ *ODS*, *ODFIM* und *InventoryScan* anhalten und fortsetzen.

Um die Aufgabe zu starten, führen Sie folgenden Befehl aus:

```
kesl-control --start-task < ID/Name der Aufgabe > [-W] [--progress]
```

Wobei gilt:

- `< ID/Name der Aufgabe >` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `[-W]` – Verwenden Sie diesen Befehl in Verbindung mit dem Befehl zum Starten der Aufgabe, wenn Sie die Ausgabe von aktuellen Ereignissen im Zusammenhang mit dieser Aufgabe aktivieren möchten.
- `[--progress]` – Geben Sie diesen Schalter an, wenn Sie den Fortschritt der laufenden Aufgabe anzeigen möchten.

  Beispiel:
  Starten Sie eine Aufgabe mit der ID 1 und aktivieren Sie die Ausgabe von aktuellen Ereignissen, die mit der Aufgabe verbunden sind:

  ```
  kesl-control --start-task 1 -W
  ```

Um die Aufgabe zu stoppen, führen Sie folgenden Befehl aus:

```
kesl-control --stop-task <ID/Name der Aufgabe> [-W]
```

Wobei gilt:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `[-W]` – Verwenden Sie diesen Befehl in Verbindung mit dem Befehl zum Beenden der Aufgabe, wenn Sie die Ausgabe von aktuellen Ereignissen im Zusammenhang mit dieser Aufgabe aktivieren möchten.

Um die Aufgabe anzuhalten, führen Sie folgenden Befehl aus:

```
kesl-control --suspend-task <ID/Name der Aufgabe>
```

Um die Aufgabe fortzusetzen, führen Sie folgenden Befehl aus:

```
kesl-control --resume-task <ID/Name der Aufgabe>
```

Aufgabe über die Befehlszeile löschen

Sie können nur Benutzeraufgaben löschen. Vordefinierte Aufgaben können nicht gelöscht werden.

Um eine Aufgabe zu löschen, führen Sie folgenden Befehl aus:

```
kesl-control --delete-task <ID/Name der Aufgabe>
```

Wobei gilt: `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Aufgabeneinstellungen über die Befehlszeile ausgeben

Sie können die aktuellen Werte der Einstellungen aller Benutzeraufgaben und aller vordefinierten Aufgaben anzeigen, mit Ausnahme der Aufgaben *Rollback* und *License* (diese Aufgaben haben keine Einstellungen).

Sie können die aktuellen Werte von Aufgabeneinstellungen in die Konsole oder in eine Konfigurationsdatei ausgeben, die Sie verwenden können, um Aufgabeneinstellungen zu ändern.

Um die aktuellen Werte der Aufgabeneinstellungen in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings <ID/Name der Aufgabe> [--json]
```

Wobei gilt:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

- `--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Um die aktuellen Werte der Aufgabeneinstellungen in eine Konfigurationsdatei auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings <ID/Name der Aufgabe> --file <Pfad der
Konfigurationsdatei> [--json]
```

Wobei gilt:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--file <Pfad der Konfigurationsdatei>` – Pfad der Konfigurationsdatei, in der die App-Einstellungen ausgegeben werden. Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.
- `--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Aufgabeneinstellungen über die Befehlszeile bearbeiten

Sie können die Einstellungen aller Benutzeraufgaben und aller vordefinierten Aufgaben ändern, mit Ausnahme der Aufgaben *Rollback* und *License*.

Wenn die App im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, können die Einstellungen der vordefinierten Aufgabe *Update* ebenfalls nicht geändert werden.

In der Befehlszeile können Sie Aufgabeneinstellungen mit dem Befehl `kesl-control --set-settings` ändern:

- Sie können alle Aufgabeneinstellungen ändern, indem Sie die Konfigurationsdatei verwenden, die die Aufgabeneinstellungen enthält. Sie können die Konfigurationsdatei mit dem Befehl zur Ausgabe der Aufgabeneinstellungen abrufen.
- Sie können einzelne Aufgabeneinstellungen mithilfe von Befehlszeilenschaltern im Format `<Name der Einstellung>=<Wert der Einstellung>` ändern. Sie können die aktuellen Werte der Aufgabeneinstellungen mit dem Befehl zur Ausgabe der Aufgabeneinstellungen abrufen.
- Sie können die Standardaufgabeneinstellungen wiederherstellen.

Sie können Untersuchungsbereiche und Ausschlussbereiche mithilfe einer Konfigurationsdatei, die Aufgabeneinstellungen oder Befehlszeilenschalter enthält, hinzufügen und entfernen. Die Konfiguration von Untersuchungsbereichen und Ausschlussbereichen ist für Aufgaben vom Typ *OAS*, *ODS*, *OAFIM*, *ODFIM* und *AntiCryptor* verfügbar.

Bei Systemen mit dem Dateisystem BTRFS und aktivierten aktiven Snapshots wird es zur Optimierung der Untersuchungsaufgaben empfohlen, den Pfad mit dem im "Read only"-Modus gemounteten Snapshots den Ausschlüssen hinzuzufügen. Beispielsweise können in Systemen auf Basis von SUSE/OpenSUSE den Pfad für die Ausschlüsse folgendermaßen angeben: `/.snapshots/*/snapshot/`.

Einige Aufgaben verfügen auch über separate Verwaltungsbefehle, mit denen Sie Aufgabeneinstellungen ändern können.

Aufgabeneinstellungen mithilfe einer Konfigurationsdatei bearbeiten

So ändern Sie die Werte der Aufgabeneinstellungen mithilfe einer Konfigurationsdatei:

1. Geben Sie die Aufgabeneinstellungen mithilfe des Befehls `kesl-control --get-schedule` in der Konfigurationsdatei aus.

2. Öffnen Sie die Konfigurationsdatei und ändern Sie die Werte der erforderlichen Einstellungen.

   Für die Aufgaben vom Typ *OAS*, *ODS*, *OAFIM*, *ODFIM* und *AntiCryptor* können Sie Untersuchungsbereiche und Ausschlussbereiche hinzufügen oder entfernen.

   Wenn Sie einen Untersuchungsbereich hinzufügen möchten, fügen Sie der Datei den Abschnitt `[ScanScope.item_#]` mit den folgenden Parametern hinzu:

   - `AreaDesc` – Beschreibung des Untersuchungsbereichs, die zusätzliche Informationen zu diesem Bereich enthält.
   - `UseScanArea` – Aktiviert die Untersuchung des angegebenen Bereichs.
   - `Path` – Pfad zum Verzeichnis mit untersuchten Objekten. Sie können den Pfad zu einem lokalen Verzeichnis angeben oder die Untersuchung von Remote-Verzeichnissen aktivieren, die auf dem Client-Gerät eingebunden sind.
   - `AreaMask.item_#` – Einschränkung des Untersuchungsbereichs. Sie können eine Maske für die Namen der zu scannenden Dateien festlegen. Standardmäßig ist die Untersuchung für alle Objekte im Untersuchungsbereich aktiviert. Sie können mehrere Elemente vom Typ `AreaMask.item_#` angeben.

   Wenn Sie einen Ausschlussbereich hinzufügen möchten, fügen Sie der Datei den Abschnitt `[ExcludedFromScanScope.item_#]` mit den folgenden Parametern hinzu:

   - `AreaDesc` – Beschreibung des Ausschlussbereichs, die zusätzliche Informationen zum Ausschlussbereich enthält.
   - `UseScanArea` – Aktiviert den Ausschluss des angegebenen Bereichs.
   - `Path` – Pfad zum Verzeichnis mit ausgeschlossenen Objekten. Sie können den Pfad zu einem lokalen Verzeichnis angeben oder Remote-Verzeichnisse ausschließen, die auf dem Client-Gerät eingebunden sind. Mögliche Einstellungswerte hängen vom Aufgabentyp ab.
   - `AreaMask.item_#` – Einschränkung des Ausschlussbereichs. Sie können eine Maske für Namen von Dateien angeben, die Sie aus dem Untersuchungsbereich ausschließen möchten. Standardmäßig sind alle Bereichsobjekte ausgeschlossen.

     Beispiel:
     ```
     [ExcludedFromScanScope.item_0000]
     AreaDesc=
     ```

```
UseScanArea=Yes
Path=/tmp/notchecked
AreaMask.item_0000=*
```

Sie können mehrere Abschnitte vom Typ `[ScanScope.item_#]` und `[ExcludedFromScanScope.item_#]` angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge.

3. Speichern Sie die Konfigurationsdatei.

4. Führen Sie den Befehl aus:

   `kesl-control --set-settings <ID/Name der Aufgabe> --file <Pfad der Konfigurationsdatei> [--json]`

   Wobei gilt:

   - `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
   - `--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die Einstellungen der Aufgabe importiert werden.
   - `--json` – Geben Sie diesen Schalter an, wenn Sie Einstellungen aus einer Konfigurationsdatei im JSON-Format importieren. Wenn Sie den Schalter `--json` nicht angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Alle in der Datei angegebenen Werte der Aufgabeneinstellungen werden in die App importiert.

Wenn Sie in den Einstellungen der Aufgabe App-Kontrolle die Liste mit erlaubten Apps ändern oder den Start aller Apps und/oder der Apps, welche die Ausführung von Kaspersky Endpoint Security beeinflussen, verbieten, müssen Sie den Befehl `--set-settings` mit dem Schalter `--accept` ausführen.

Aufgabeneinstellungen mithilfe der Befehlszeilenschalter bearbeiten

Mit den Befehlsschaltern `kesl-control --set-settings` können Sie einzelne Werte der Aufgabeneinstellungen ändern sowie Untersuchungsbereiche und Ausschlussbereiche für Aufgaben vom Typ *OAS*, *ODS*, *OAFIM*, *ODFIM* und *AntiCryptor* hinzufügen oder entfernen.

Einzelne Aufgabeneinstellungen konfigurieren

Um einzelne Werte der Aufgabeneinstellungen mithilfe von Befehlszeilenschaltern zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings <ID/Name der Aufgabe> <Name der Einstellung>=<Wert der Einstellung> [<Name der Einstellung>=<Wert der Einstellung>]
```

Wobei gilt:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

- `<Name der Einstellung>=<Wert der Einstellung>` – Name und Wert einer der Aufgabeneinstellungen. Sie können die aktuellen Werte der Aufgabeneinstellungen mit dem Befehl zur Ausgabe der Aufgabeneinstellungen abrufen.

Die Werte der angegebenen Aufgabeneinstellungen werden geändert.

Wenn Sie in den Einstellungen der Aufgabe App-Kontrolle die Liste mit erlaubten Apps ändern oder den Start aller Apps und/oder der Apps, welche die Ausführung von Kaspersky Endpoint Security beeinflussen, verbieten, müssen Sie den Befehl `--set-settings` mit dem Schalter `--accept` ausführen.

Einen Untersuchungsbereich hinzufügen oder entfernen

Um einen Untersuchungsbereich mithilfe von Befehlszeilenschaltern hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings <ID/Name der Aufgabe> --add-path <Pfad>
```

Wobei gilt:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--add-path <Pfad>` – Fügen Sie den Pfad zum Verzeichnis mit den untersuchten Objekten hinzu.

Den Aufgabeneinstellungen wird ein neuer Abschnitt vom Typ `[ScanScope.item_#]` hinzugefügt. Die App untersucht die Objekte im Verzeichnis, das im Parameter `Path` angegeben ist. Die übrigen Einstellungen für den Untersuchungsbereich nehmen Standardwerte an.

Wenn in den Aufgabeneinstellungen bereits ein Abschnitt vom Typ `[ScanScope.item_#]` mit dem angegebenen Einstellungswert `Pfad` existiert, wird der Abschnitt nicht dupliziert.

Wenn die Einstellung `UseScanArea` der Wert `No` besaß, ändert sich der Wert nach der Ausführung dieses Befehls zu `Yes` und die Objekte, die sich in diesem Verzeichnis befinden, werden untersucht.

Beispiel:
Hinzufügen eines Untersuchungsbereichs für eine Aufgabe mit der ID=100:

```
kesl-control --set-settings 100 ScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/home
```

Die folgenden Einstellungen für den Untersuchungsbereich werden der Aufgabe hinzugefügt:

```
[ScanScope.item_0001]

AreaDesc=

UseScanArea=Yes

Path=/home
```

```
AreaMask.item_0000=*
```

Um einen Untersuchungsbereich mithilfe von Befehlszeilenschaltern zu entfernen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings <ID/Name der Aufgabe> --del-path <Pfad>
```

Wobei gilt:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--del-path <Pfad>` – Löscht den Pfad zum Verzeichnis mit den untersuchten Objekten.

Der Abschnitt `[ScanScope.item_#]`, der den angegebenen Pfad enthält, wird aus den Aufgabeneinstellungen entfernt. Die App untersucht keine der Objekte im angegebenen Verzeichnis.

Einen Ausschlussbereich hinzufügen oder entfernen

Um einen Ausschlussbereich mithilfe von Befehlszeilenschaltern hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings <ID/Name der Aufgabe> --add-exclusion <Pfad>
```

Wobei gilt:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--add-exclusion <Pfad>` – Fügen Sie den Pfad zum Verzeichnis mit Objekten hinzu, die Sie von der Untersuchung ausschließen möchten.

Den Aufgabeneinstellungen wird ein neuer Abschnitt vom Typ `[ExcludedFromScanScope.item_#]` hinzugefügt. Die App schließt die Objekte im Verzeichnis, das im Parameter `Path` angegeben ist, von der Untersuchung aus. Die übrigen Einstellungen für den Ausschlussbereich nehmen Standardwerte an.

Wenn in den Aufgabeneinstellungen bereits ein Abschnitt vom Typ `[ExcludedFromScanScope.item_#]` mit dem angegebenen Einstellungswert `Pfad` existiert, wird der Abschnitt nicht dupliziert.

Wenn die Einstellung `UseScanArea` den Wert `No` besaß, ändert sich der Wert nach der Ausführung dieses Befehls zu `Yes` und die Objekte, die sich in diesem Verzeichnis befinden, werden von der Untersuchung ausgeschlossen.

Um einen Ausschlussbereich mithilfe von Befehlszeilenschaltern zu entfernen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings <ID/Name der Aufgabe> --del-exclusion <Pfad>
```

Wobei gilt:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

- `--del-path <Pfad>` – Löscht den Pfad zum Verzeichnis mit den ausgeschlossenen Objekten.

  Der Abschnitt `[ExcludedFromScanScope.item_#]`, der den angegebenen Pfad enthält, wird aus den Aufgabeneinstellungen entfernt. Die App schließt keines der Objekte im angegebenen Verzeichnis von der Untersuchung aus.

Standardaufgabeneinstellungen über die Befehlszeile wiederherstellen

Sie können die Standardwerte der Einstellungen aller Benutzeraufgaben und aller vordefinierten Aufgaben wiederherstellen, mit Ausnahme der Aufgaben vom Typ *Rollback* und *License* (diese Aufgaben haben keine Einstellungen).

Um die Standardaufgabeneinstellungen über die Befehlszeile wiederherzustellen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings <ID/Name der Aufgabe> --set-to-default
```

Wobei gilt: `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Die App setzt die Werte der Einstellungen auf die Standardwerte zurück.

Aufgabenzeitplan über die Befehlszeile anpassen

Wenn die App im Standard-Modus verwendet wird, können Sie einen Zeitplan für den Start von Aufgaben der folgenden Typen erstellen: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* und *InventoryScan*.

Wenn die App im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, können Sie einen Zeitplan für den Start von Aufgaben der folgenden Typen erstellen: *ODS*, *ODFIM*, *ContainerScan* und *InventoryScan*.

Sie können die aktuellen Werte für die Einstellungen des Zeitplans für den Aufgabenstart in die Konsole oder in eine Konfigurationsdatei ausgeben.

Um die aktuellen Einstellungen des Zeitplans für den Aufgabenstart in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-schedule <ID/Name der Aufgabe> [--json]
```

Wobei gilt:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Um die aktuellen Einstellungen des Zeitplans für den Aufgabenstart in die Konfigurationsdatei auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-schedule <ID/Name der Datei> --file <Pfad der Konfigurationsdatei>
[--json]
```

Wobei gilt:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--file <Pfad der Konfigurationsdatei>` – Pfad der Konfigurationsdatei, in der die Einstellungen für den Aufgabenzeitplan ausgegeben werden. Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.
- `--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

  Beispiele:
  So speichern Sie die Einstellungen der Update-Aufgabe in einer neu erstellten Datei mit dem Namen update_schedule.ini im aktuellen Verzeichnis:

  ```
  kesl-control --get-schedule 6 --file update_schedule.ini
  ```

  So geben Sie den Zeitplan der Update-Aufgabe in die Konsole aus:

  ```
  kesl-control --get-schedule 6
  ```

Sie können die Einstellungen des Zeitplans für den Aufgabenstart wie folgt ändern:

- Importieren Sie die Einstellungen aus einer Konfigurationsdatei, die alle Zeitplaneinstellungen enthält.
- Geben Sie über die Befehlszeile die einzelnen Einstellungen des Zeitplans für den Aufgabenstart im Format `<Name der Einstellung>=<Wert der Einstellung>` ein.

Gehen Sie folgendermaßen vor, um die Werte der Einstellungen des Zeitplans für den Aufgabenstart mithilfe einer Konfigurationsdatei zu ändern:

1. Geben Sie die Aufgabeneinstellungen mithilfe des Befehls `kesl-control --get-schedule` in der Konfigurationsdatei aus.
2. Ändern Sie die Werte der erforderlichen Einstellungen in der Datei und speichern Sie die Änderungen.
3. Führen Sie den Befehl aus:

   ```
   kesl-control --set-schedule <ID/Name der Datei> --file <Pfad der Konfigurationsdatei>
   [--json]
   ```

   Wobei gilt:

   `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

   `--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die Einstellungen des Aufgabenzeitplans importiert werden.

   `--json` – Geben Sie diesen Schalter an, wenn Sie Einstellungen aus einer Konfigurationsdatei im JSON-Format importieren. Wenn Sie den Schalter `--json` nicht angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Alle in der Datei angegebenen Werte der Einstellungen des Zeitplans für den Aufgabenstart werden in die App importiert.

Beispiel:
Zeitplaneinstellungen aus der Konfigurationsdatei /home/test/on_demand_schedule.ini in die Aufgabe mit ID=2 importieren:

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

Um einzelne Werte der Einstellungen des Zeitplans für den Aufgabenstart mithilfe der Befehlszeile zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-schedule <ID/Name der Aufgabe> <Name der Einstellung>=<Wert der Einstellung> [<Name der Einstellung>=<Wert der Einstellung>]
```

Wobei gilt:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `<Name der Einstellung>=<Wert der Einstellung>` – Name und Wert einer der Einstellungen des Aufgabenzeitplans.

Die Werte der angegebenen Einstellungen des Zeitplans für den Aufgabenstart werden geändert.

Beispiele:
Geben Sie die folgenden Einstellungen an, damit die Aufgabe nach Zeitplan alle zehn Stunden gestartet wird:

```
RuleType=Hourly

RunMissedStartRules=No

StartTime=2021/May/30 23:05:00;10

RandomInterval=0
```

Geben Sie die folgenden Einstellungen an, damit die Aufgabe nach Zeitplan alle zehn Minuten gestartet wird:

```
RuleType=Minutely

RunMissedStartRules=No

StartTime=23:10:00;10

RandomInterval=0
```

Geben Sie die folgenden Einstellungen an, damit die Aufgabe nach Zeitplan am 15. jeden Monats gestartet wird:

```
RuleType=Monthly
```

```
RunMissedStartRules=No

StartTime=23:25:00;15

RandomInterval=0
```

Geben Sie die folgenden Einstellungen an, damit die Aufgabe nach Zeitplan jeden Dienstag gestartet wird:

```
RuleType=Weekly

StartTime=18:01:30;Tue

RandomInterval=99

RunMissedStartRules=No
```

Geben Sie die folgenden Einstellungen an, damit die Aufgabe nach Zeitplan alle 11 Tage gestartet wird:

```
RuleType=Daily

RunMissedStartRules=No

StartTime=23:15:00;11

RandomInterval=0
```

Allgemeine App-Einstellungen über die Befehlszeile verwalten

Die allgemeinen App-Einstellungen bestimmen die Ausführung der App als Ganzes und die Ausführung einzelner Funktionen.

Sie können die allgemeinen App-Einstellungen mithilfe spezieller Verwaltungsbefehle verwalten:

- Geben Sie die aktuellen Werte der allgemeinen App-Einstellungen in die Konsole oder in eine Konfigurationsdatei aus.
- Ändern Sie allgemeine App-Einstellungen mithilfe einer Konfigurationsdatei, die alle allgemeinen Einstellungen enthält, oder mithilfe von Befehlszeilenschaltern im Format < `Name der Einstellung` >=< `Wert der Einstellung` >.

Mit den allgemeinen Einstellungen können Sie Folgendes tun:

- Konfigurieren Sie die Verwendung von Kaspersky Security Network und einer schlankeren Version der Malware-Datenbanken in der App.
- Konfigurieren Sie die Verwendung eines Proxy-Servers in der App.
- Konfigurieren Sie den Modus des Moduls zum Abfangen von Dateioperationen (Dateien während der Untersuchung blockieren/nicht blockieren).

- Konfigurieren Sie Ausschlüsse von der Untersuchung von Mountpunkten (globale Ausschlüsse).
- Konfigurieren Sie Ausschlüsse von der Untersuchung des Arbeitsspeichers.
- Aktivieren und deaktivieren Sie die Untersuchung von Containern in Echtzeit.
- Aktivieren und deaktivieren Sie die Erkennung von legitimen Apps, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können.
- Aktivieren und deaktivieren Sie die Integration mit Kaspersky Managed Detection and Response.
- Konfigurieren Sie die Verwendung von Ereignisprotokollen.
- Konfigurieren Sie eine Begrenzung der Nutzung von CPU-Ressourcen für Untersuchungsaufgaben (z. B. vom Typ ODS).
- Begrenzen Sie die Anzahl der benutzerdefinierten Untersuchungsaufgaben, die ein nicht privilegierter Benutzer gleichzeitig ausführen kann.

Allgemeine App-Einstellungen ausgeben

Sie können die aktuellen Werte der allgemeinen App-Einstellungen in die Konsole oder in eine Konfigurationsdatei ausgeben, die Sie verwenden können, um Aufgabeneinstellungen zu ändern.

Um die aktuellen Werte der allgemeinen App-Einstellungen in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-app-settings [--json]
```

Wobei gilt: `--json` – Gibt Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Um die aktuellen Werte der allgemeinen App-Einstellungen in eine Konfigurationsdatei auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-app-settings --file <Pfad der Konfigurationsdatei> [--json]
```

Wobei gilt:

- `--file <Pfad der Konfigurationsdatei>` – Pfad der Konfigurationsdatei, in der die allgemeinen App-Einstellungen ausgegeben werden. Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.
- `--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

  Beispiel:
  Die allgemeinen App-Einstellungen in eine Datei mit dem Namen kesl_config.ini ausgeben. Erstellte Datei im aktuellen Verzeichnis speichern:
  ```
  kesl-control --get-app-settings --file kesl_config.ini
  ```

Allgemeine App-Einstellungen ändern

In der Befehlszeile können Sie die allgemeinen App-Einstellungen mit dem Befehl `kesl-control --set-app-settings` ändern:

- Sie können alle allgemeinen Einstellungen ändern, indem Sie die Konfigurationsdatei verwenden, die die allgemeinen App-Einstellungen enthält. Sie können die Konfigurationsdatei mit dem Befehl zur Ausgabe der allgemeinen Einstellungen abrufen.
- Sie können einzelne Einstellungen mithilfe von Befehlszeilenschaltern im Format `<Name der Einstellung>=<Wert der Einstellung>` ändern. Sie können die aktuellen Werte der allgemeinen Einstellungen mit dem Befehl zur Ausgabe der allgemeinen Einstellungen abrufen.

So ändern Sie die Werte der allgemeinen Einstellungen mithilfe einer Konfigurationsdatei:

1. Geben Sie die allgemeinen App-Einstellungen in eine Konfigurationsdatei aus.
2. Ändern Sie die Werte der erforderlichen Einstellungen in der Datei und speichern Sie die Änderungen.
3. Führen Sie den Befehl aus:

   `kesl-control --set-app-settings --file <Pfad der Konfigurationsdatei> [--json]`

   Wobei gilt:

   - `--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei mit den allgemeinen App-Einstellungen.
   - `--json` – Geben Sie diesen Schalter an, wenn Sie Einstellungen aus einer Konfigurationsdatei im JSON-Format importieren. Wenn Sie den Schalter `--json` nicht angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

   Alle in der Datei angegebenen Werte der allgemeinen Einstellungen werden in die App importiert.

Um die Werte der allgemeinen Einstellungen mithilfe von Befehlszeilenschaltern zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings <Name der Einstellung>=<Wert der Einstellung> [<Name der Einstellung>=<Wert der Einstellung>]
```

Wobei gilt: `<Name der Einstellung>=<Wert der Einstellung>` – Name und Wert einer der allgemeinen App-Einstellungen.

Die Werte der angegebenen allgemeinen Einstellungen werden geändert.

Beispiele:

Allgemeine Einstellungen aus der Konfigurationsdatei /home/test/kesl_config.ini in die App importieren:

```
kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

Niedrigen Detaillierungsgrad für die Protokolldatei festlegen:

```
kesl-control --set-app-settings TraceLevel=NotDetailed
```

Fügen Sie den Mountpunkt hinzu, den Sie vom Modul zum Abfangen von Dateioperationen ausschließen möchten:

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/data"
```

Filter zur Eingrenzung der Abfrageergebnisse verwenden

Mit einem Filter können Sie die Ergebnisse einer Abfrage beim Ausführen von Befehlen zur App-Verwaltung eingrenzen.

Filterbedingungen werden mithilfe eines oder mehrerer *logischer Ausdrücke* angegeben, die mit dem logischen Operator `and` kombiniert werden. Filterbedingungen müssen in Anführungszeichen gesetzt werden:

`"<Feld> <Vergleichsoperator> '<Wert>'"`

`"<Feld> <Vergleichsoperator> '<Wert>' and <Feld> <Vergleichsoperator> '<Wert>'"`

Wobei gilt:

- `<Feld>` – Name des Datenbankfelds.
- `<Vergleichsoperator>` – Einer der folgenden Vergleichsoperatoren:
  - `>` – Größer als.
  - `<` – Kleiner als.
  - `like` – Entspricht dem angegebenen Wert. Bei der Angabe eines Wertes können Sie %-Masken verwenden, zum Beispiel: Der logische Ausdruck "FileName like '%etc%'" gibt die Bedingung "enthält 'etc' im FileName-Feld" an.
  - `==` – Ist gleich.
  - `!=` – Ist ungleich.
  - `>=` – Größer oder gleich.
  - `<=` – Kleiner oder gleich.
- `<Wert>` – Feldwert. Der Wert muss in einfachen Anführungszeichen (') angegeben werden.

  Sie können den Datumswert als Unix-Zeitstempel (Anzahl der vergangenen Sekunden seit 1. Januar 1970, 00:00:00 Uhr (UTC)) oder im Format JJJJ-MM-TT hh:mm:ss angeben. Der Datums- und Uhrzeitwert wird vom Benutzer angegeben und von der App in der Ortszeit des Benutzers angezeigt.

Sie können den Filter in den folgenden Befehlen zur App-Verwaltung verwenden:

- Abrufen von Informationen zu bestimmten aktuellen App-Ereignissen:

  `kesl-control -W --query "<Filterbedingungen>"`
- Abrufen von Informationen zu bestimmten App-Ereignissen im Ereignisprotokoll:

  `kesl-control -E --query "<Filterbedingungen>"`
- Abrufen von Informationen zu bestimmten Objekten im Backup:

```
kesl-control -B --query "< Filterbedingungen >"
```

- Löschen bestimmter Objekte aus dem Backup:

  ```
  kesl-control -B --mass-remove --query "< Filterbedingungen >"
  ```

  Beispiele:
  Abrufen von Informationen zu Ereignissen, die den Text "etc" im Feld "FileName" enthalten:
  `kesl-control -E --query "FileName like '%etc%'"`
  Abrufen von Ereignissen vom Typ "ThreatDetected" (Bedrohung erkannt):
  `kesl-control -E--query "EventType == 'ThreatDetected'"`
  Abrufen von Informationen zu Ereignissen vom Typ "ThreatDetected", die von Aufgaben des Typs "ODS" generiert wurden:
  `kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"`
  Abrufen von Informationen zu Ereignissen, die nach einem bestimmten Datum generiert wurden (Angabe im Zeitformat UNIX™, d. h. der Anzahl an Sekunden, die seit 00:00:00 (UTC), 1. Januar 1970 vergangen sind):
  `kesl-control -E --query "Date > '1583425000'"`
  Abrufen von Informationen zu Ereignissen, die nach dem im Format "JJJJ-MM-TT hh:mm:ss" angegebenen Datum generiert wurden:
  `kesl-control -E --query "Date > '2022-12-22 18:52:45'"`
  Abrufen von Informationen zu Dateien im Backup mit der Signifikanz "High":
  `kesl-control -B --query "DangerLevel == 'High'"`

App-Einstellungen exportieren und importieren

Wenn Sie Kaspersky Endpoint Security mithilfe von Kaspersky Security Center verwalten, ist der Import von Einstellungen nicht verfügbar.

Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, können die Einstellungen der vordefinierten Aufgabe vom Typ *Update* nicht exportiert oder importiert werden.

In Kaspersky Endpoint Security können zur Fehlerbehebung, Überprüfung der Einstellungen oder zur einfacheren Konfiguration der App auf Benutzergeräten alle App-Einstellungen exportiert und importiert werden. Wenn Sie Einstellungen exportieren, werden alle App-Einstellungen (einschließlich der allgemeinen Einstellungen der Container-Untersuchung, der Einstellungen zur Untersuchung geschützter Verbindungen, der allgemeinen App-Einstellungen und der Aufgabeneinstellungen) in der Konfigurationsdatei gespeichert. Sie können diese Konfigurationsdatei verwenden, um Einstellungen in die App zu importieren.

Während des Imports und Exports von Einstellungen muss die App ausgeführt werden. Nach dem Import der Einstellungen ist ein Neustart der App erforderlich.

Beim Importieren oder Exportieren von Einstellungen aus älteren Versionen der App, werden für neue Einstellungen die Standardwerte verwendet. Das Importieren von Einstellungen in eine ältere Version der App ist nicht möglich.

Um App-Einstellungen zu exportieren, führen Sie den folgenden Befehl aus:

```
kesl-control --export-settings --file < Pfad der Konfigurationsdatei > [--json]
```

Wobei gilt:

- `--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, in der die App-Einstellungen gespeichert werden.
- `--json` – Exportiert Einstellungen in eine Konfigurationsdatei im JSON-Format. Wenn Sie den Schalter `--json` nicht angeben, erfolgt der Export in eine Datei im INI-Format.

Um App-Einstellungen aus einer Datei zu importieren, führen Sie den folgenden Befehl aus:

```
kesl-control --import-settings --file <Pfad der Konfigurationsdatei> [--json]
```

Wobei gilt:

- `--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die Parameter in die App importiert werden.
- `--json` – Importiert die Einstellungen aus einer Konfigurationsdatei im JSON-Format. Wenn Sie den Schalter `--json` nicht angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Beim Import von Parametern aus einer Datei wird für die Parameter `UseKSN` und `CloudMode` den Wert `No` vergeben. Um die Verwendung von Kaspersky Security Network zu beginnen oder fortzusetzen, müssen Sie für den Parameter `UseKSN` den Wert `Basic` oder `Extended` festlegen. Um den Cloud-Modus zu aktivieren, müssen Sie für den Parameter `CloudMode` den Wert `Yes` festlegen. Der Cloud-Modus ist verfügbar, wenn KSN aktiviert ist.

Durch den Import der App-Einstellungen können sich die internen Aufgaben-IDs ändern. Es wird empfohlen, zur Aufgabenverwaltung die Aufgabennamen zu verwenden.

Benutzerrollen über die Befehlszeile verwalten

Benutzer können entsprechend ihren Rollen über die Befehlszeile auf die Funktionen von Kaspersky Endpoint Security zugreifen. *Rolle* – Eine Reihe von Rechten und Berechtigungen zur Verwaltung der App.

Im Betriebssystem werden vier Gruppen mit Systembenutzern erstellt: *kesladmin*, *kesluser*, *keslaudit* und *nokesl*. Wenn eine Rolle der App einem Benutzer des Systems zugewiesen wird, wird der Benutzer zur entsprechenden Gruppe für die Rolle hinzugefügt (s. nachfolgende Tabelle *Rollen*). Wenn Sie einem Benutzer eine Rolle entziehen, wird dieser Benutzer aus der entsprechenden Rollengruppe entfernt.

Wenn einem Systembenutzer keine Rolle für die App zugewiesen wurde, gehört dieser Benutzer zur entsprechenden Gruppe *Benutzer ohne Berechtigungen*.

Somit entsprechen die Rollen vier Gruppen von Benutzern des Betriebssystems:

- kesladmin entspricht der Rolle "Administrator".
- kesluser entspricht der Rolle "Benutzer".
- keslaudit entspricht der Rolle "Auditor".

- nokesl wird einem Benutzer zugewiesen, dem keine andere Rolle zugewiesen ist. In diesem Fall gehört der Benutzer zu einer spezifischen Gruppe der *Benutzer ohne Berechtigungen*.

Benutzerrollen

Rollenname	Rolle für die App	Benutzer des Betriebssystems	Berechtigungen
Administrator	admin	kesladmin	Verwaltung der App- und Aufgabeneinstellungen Verwaltung der Lizenzierung der App beliebigen Benutzern beliebige Rollen zuweisen beliebigen Benutzern beliebige Rollen entziehen (der Administrator kann sich die Rolle admin nicht selbst entziehen) Benutzerspeicher anzeigen und verwalten
Benutzer	Benutzer	kesluser	Nur Aufgaben für die benutzerdefinierte Untersuchung von Dateien verwalten Update-Aufgaben starten und beenden Berichte für von Benutzern erstellte Aufgaben anzeigen Anzeigen von Ereignissen, die für alle Benutzer der App gelten
Auditor	audit	keslaudit	Einstellungen der App anzeigen Status der App anzeigen Alle Aufgaben samt Einstellungen und Zeitplänen anzeigen Alle Ereignisse anzeigen Alle Objekte im Backup anzeigen
—	–	nokesl	Keine Rolle in der App zugewiesen, es gibt keine Rechte.

Liste von Benutzern und Rollen anzeigen

Um eine Liste der Benutzer und deren Rollen anzuzeigen, führen Sie folgenden Befehl aus:

```
kesl-control [-U] --get-user-list
```

Einem Benutzer eine Rolle zuweisen

Um einem bestimmten Benutzer eine Rolle zuzuweisen, führen Sie folgenden Befehl aus:

```
kesl-control [-U] --grant-role <Rolle> <Benutzer>
```

Beispiel:
So weisen Sie dem Benutzer test15 die Rolle "audit" zu:

```
kesl-control --grant-role audit test15
```

Einem Benutzer eine Rolle entziehen

Um einem bestimmten Benutzer eine Rolle zu entziehen, führen Sie folgenden Befehl aus:

```
kesl-control [-U] --revoke-role <Rolle> <Benutzer>
```

Beispiel:
So entziehen Sie dem Benutzer test15 die Rolle "audit":

```
kesl-control --revoke-role audit test15
```

App starten und beenden

Nach der Installation von Kaspersky Endpoint Security auf dem Gerät wird die App automatisch gestartet. Danach wird die App standardmäßig automatisch gestartet, wenn das Betriebssystem hochfährt (innerhalb der Standardausführungsebene für jedes Betriebssystem).

Standardmäßig werden beim Start von Kaspersky Endpoint Security automatisch die folgenden Funktionskomponenten der App gestartet:

- Schutz vor bedrohlichen Dateien.
- Gerätekontrolle.
- Verhaltensanalyse.
- Schutz vor Web-Bedrohungen – Nur wenn einer der unterstützten Browser im Betriebssystem installiert ist und die lokale Verwaltung der Einstellungen für den Schutz vor Web-Bedrohungen auf dem Gerät zugelassen ist (die Richtlinie wird nicht angewendet oder das "Schloss" ist in den Eigenschaften der Richtlinie nicht gesetzt).
- Schutz vor Netzwerkbedrohungen – Nur wenn die Einstellungen für den Schutz vor Netzwerkbedrohungen auf dem Gerät durch eine Richtlinie festgelegt werden. Standardmäßig ist in den Eigenschaften die Richtlinie der Schutz vor Netzwerkbedrohungen aktiviert. Wenn auf das Gerät lokal konfigurierte Einstellungen angewendet werden, ist der Schutz vor Netzwerkbedrohungen standardmäßig deaktiviert.

Wenn Sie die App auf dem Gerät starten, werden automatisch Dienstaufgaben gestartet, um die Ausführung zusätzlicher App-Funktionen sicherzustellen: Funktionen zur App-Aktivierung und Backup-Funktionen.

Standardmäßig führt die App auch Benutzeraufgaben aus, die in der Befehlszeile konfiguriert sind und die gemäß Startmodus nach dem Start der App ausgeführt werden sollen (Startmodus `PS`).

Wenn Sie die App beenden, werden alle momentan auf dem Gerät laufenden Aufgaben unterbrochen. Unterbrochene Benutzeraufgaben werden nach dem Neustart der App nicht automatisch fortgesetzt.

App mithilfe von Web Console starten und beenden

So starten oder beenden Sie die App aus der Ferne:

1. Wählen Sie im Hauptfenster der Web Console die Option **Assets (Geräte)** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie in der Liste das Gerät aus, auf dem Sie die App starten oder stoppen möchten, und klicken Sie auf den Link mit dem Namen des Geräts, um das Eigenschaftenfenster des Geräts zu öffnen.
3. Wählen Sie die Registerkarte **Anwendungen** aus.
4. Aktivieren Sie das Kontrollkästchen neben **Kaspersky Endpoint Security 12.1 für Linux**.
5. Führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie die App starten möchten, klicken Sie auf die Schaltfläche **Starten**.
   - Wenn Sie die App beenden möchten, klicken Sie auf die Schaltfläche **Beenden**.

Sie können den Status der App-Ausführung mithilfe des Web-Widgets **Schutzstatus** im Fenster **Überwachung und Berichterstattung / Dashboard "Überwachung"** überwachen.

App mithilfe der Verwaltungskonsole starten und beenden

So starten oder beenden Sie die App auf einem Client-Gerät:

1. Wählen Sie in der Struktur der Verwaltungskonsole im Ordner **Verwaltete Geräte** die Administrationsgruppe aus, die das benötigte Gerät enthält.
2. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.
3. Wählen Sie in der Liste der verwalteten Geräte das Gerät aus, auf dem Sie die App starten oder stoppen möchten, und wählen Sie **Eigenschaften** aus dem Kontextmenü des Geräts.
4. Wählen Sie im Fenster **Eigenschaften: <App-Name>** den Abschnitt **Programme**.

   Im rechten Teil des Fensters wird eine Liste der auf dem Gerät installierten Apps von Kaspersky angezeigt.
5. Wählen Sie **Kaspersky Endpoint Security 12.1 für Linux** aus.
6. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie die App ausführen möchten, klicken Sie auf die Schaltfläche  rechts neben der Liste der Kaspersky-Apps oder wählen Sie im Kontextmenü der App den Punkt **Starten**.
   - Wenn Sie die App beenden möchten, klicken Sie auf die Schaltfläche  rechts neben der Liste der Kaspersky-Apps oder wählen Sie im Kontextmenü der App den Punkt **Stoppen**.

App über die Befehlszeile starten und beenden

Um die App zu starten, muss für die folgenden Verzeichnisse das root-Benutzerkonto der Besitzer ist und ausschließlich der Besitzer Schreibrechte für diese besitzt: /var, /var/opt, /var/opt/kaspersky, /var/log/kaspersky, /opt, /opt/kaspersky, /usr/bin, /usr/lib, /usr/lib64.

Kaspersky Endpoint Security starten, neu starten und beenden

Um die App zu starten, führen Sie folgenden Befehl aus:

```
systemctl start kesl
```

Um die App zu stoppen, führen Sie folgenden Befehl aus:

```
systemctl stop kesl
```

Um die App erneut zu starten, führen Sie folgenden Befehl aus:

```
systemctl restart kesl
```

Überwachen des Status von Kaspersky Endpoint Security

Der App-Status von Kaspersky Endpoint Security wird vom Dienst Watchdog überwacht. Der Dienst Watchdog wird beim Start der App automatisch gestartet.

Sollte die App abstürzen, wird eine Dump-Datei erzeugt und die App wird automatisch neu gestartet.

Um den App-Status auszugeben, führen Sie den folgenden Befehl aus:

```
systemctl status kesl
```

Schutzstatus des Geräts und App-Einstellungen anzeigen

Sie können Informationen zum Schutzstatus des Geräts und zum Ausführungsstatus von Kaspersky Endpoint Security und seiner Komponenten auf dem Gerät anzeigen.

Sie können Informationen über den Schutzstatus des Geräts auf folgende Arten abrufen:

- In der Web Console oder in der Verwaltungskonsole mithilfe der Status der Client-Geräte (*OK*, *Kritisch*, *Warnung*). Das Gerät, auf dem der Kaspersky Security Center Administrationsagent installiert ist, ist ein Client-Gerät für Kaspersky Security Center. Der Status eines Client-Geräts kann sich aus folgenden Gründen in *Kritisch* oder *Warnung* ändern:

  - Gemäß den in Kaspersky Security Center definierten Regeln. Der Status ändert sich beispielsweise, wenn auf dem Gerät keine Schutz-App installiert ist, eine Virenprüfung längere Zeit nicht durchgeführt wurde, die App-Datenbanken veraltet sind, die Lizenz abgelaufen ist oder die App nicht stabil ausgeführt wird. Weitere Informationen zu den Gründen für Statusänderungen und zum Festlegen der Bedingungen für die Zuweisung von Status finden Sie in der Hilfe zu Kaspersky Security Center.

  - Kaspersky Security Center empfängt den Gerätestatus von der verwalteten App, also von Kaspersky Endpoint Security.

    Der Empfang eines Gerätestatus von einer verwalteten App muss in Kaspersky Security Center in den Listen der Bedingungen für die Zuweisung der Status *Kritisch* und *Warnung* aktiviert sein. Die Bedingungen für die Zuweisung von Gerätestatus werden im Eigenschaftenfenster der Administrationsgruppe konfiguriert.

  Weitere Informationen zu den Status von Client-Geräten finden Sie in der Hilfe zu Kaspersky Security Center.

- In der Web Console oder in der Verwaltungskonsole mithilfe der Status der Funktionskomponenten von Kaspersky Endpoint Security auf dem Gerät. In den Eigenschaften der auf dem Gerät installierten App Kaspersky Endpoint Security wird eine Liste der Funktionskomponenten der App angezeigt. Für jede Komponente wird ihr Status angezeigt.

- Über die Befehlszeile mit dem Befehl `kesl-control --app-info`. Der Befehl zeigt Informationen über die Ausführung der App und den Status der Funktionskomponenten und Aufgaben der App an.

Schutzstatus des Geräts in der Web Console anzeigen

So zeigen Sie den Schutzstatus des Geräts in der Web Console an:

1. Wählen Sie im Hauptfenster der Web Console die Option **Assets (Geräte)** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** oberhalb der Liste der verwalteten Geräte und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

   In der Liste werden nur die verwalteten Geräte der ausgewählten Administrationsgruppe angezeigt.

3. Suchen Sie in der Liste das Gerät, für das Sie Informationen anzeigen möchten, und klicken Sie auf den Gerätenamen.

4. Wählen Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts auf der Registerkarte **Allgemein** den Abschnitt **Schutz** aus.

Im Abschnitt **Schutz** werden folgende Informationen über das Gerät angezeigt:

- **Sichtbar im Netzwerk** – Sichtbarkeit des ausgewählten Geräts im Netzwerk: *Ja* oder *Nein*.
- **Gerätestatus** – Status des Client-Geräts, der auf der Grundlage der vom Administrator festgelegten Kriterien für den Schutzstatus auf dem ausgewählten Gerät und die Aktivität des Geräts im Netzwerk generiert wird: *OK*, *Kritisch* oder *Warnung*.
- **Statusbeschreibung** – Ursachen für die Änderung des Gerätestatus zu *Kritisch* oder *Warnung*.
- **Schutzstatus** – Aktueller Status des Schutzes vor bedrohlichen Dateien auf dem ausgewählten Gerät, z. B.: *Wird ausgeführt*, *Beendet*, *Angehalten*.
- **Letzte vollständige Untersuchung** – Datum und Uhrzeit der letzten Durchführung einer vollständigen Untersuchung auf dem ausgewählten Gerät.
- **Virus gefunden** – Gesamtmenge der bösartigen Objekte, die seit dem Installationsdatum der App Kaspersky Endpoint Security auf dem ausgewählten Gerät gefunden wurden (Zähler der gefundenen Bedrohungen).
- **Objekte, die nicht desinfiziert werden konnten** – Anzahl der infizierten Objekte, die von der App Kaspersky Endpoint Security nicht desinfiziert werden konnten.

Schutzstatus des Geräts in der Verwaltungskonsole anzeigen

So zeigen Sie den Schutzstatus des Geräts in der Verwaltungskonsole an:

1. Wählen Sie in der Struktur der Verwaltungskonsole im Ordner **Verwaltete Geräte** die Administrationsgruppe aus, die das benötigte Gerät enthält.
2. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.
3. Wählen Sie in der Liste der verwalteten Geräte das erforderliche Gerät aus und öffnen Sie das Fenster **Eigenschaften: <Gerätename>** mit einem Doppelklick.
4. Wählen Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts den Abschnitt **Schutz** aus.

Im Abschnitt **Schutz** werden folgende Informationen über das Gerät angezeigt:

- **Gerätestatus** – Status des Client-Geräts, der auf der Grundlage der vom Administrator festgelegten Kriterien für den Schutzstatus auf dem Gerät und die Aktivität des Geräts im Netzwerk generiert wird.
- **Alle Probleme** – Vollständige Liste der Probleme, die von den verwalteten Apps erkannt wurden, die auf dem Client-Gerät installiert sind. Jedes Problem hat einen Status, den Ihnen die App vorschlägt, dem Gerät zuzuweisen.
- **Status des Echtzeitschutzes** – Aktueller Status des Schutzes vor bedrohlichen Dateien auf dem ausgewählten Gerät, z. B. *Wird ausgeführt* oder *Beendet*. Wenn sich der Schutzstatus auf dem Gerät ändert, wird der neue Status erst dann im Eigenschaftenfenster des Geräts angezeigt, sobald das Client-Gerät mit dem Administrationsserver synchronisiert wird.

- **Letzte Untersuchung auf Befehl** – Datum und Uhrzeit der letzten Schadsoftware-Untersuchung auf dem ausgewählten Gerät.
- **Insgesamt gefundene Bedrohungen** – Gesamtzahl der Bedrohungen, die seit der Installation der App (seit der ersten Untersuchung des Geräts) oder seit dem letzten Zurücksetzen des Zählers auf dem ausgewählten Gerät gefunden wurden.

  Um den Zähler zurückzusetzen, klicken Sie auf die Schaltfläche **Zurücksetzen**.
- **Aktive Bedrohungen** – Die Anzahl unverarbeiteter Dateien auf dem ausgewählten Gerät.

Informationen über die Ausführung der App in der Web Console anzeigen

So zeigen Sie Informationen über die Ausführung der App in der Web Console an:

1. Wählen Sie im Hauptfenster der Web Console die Option **Assets (Geräte)** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird geöffnet.
2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** über der Liste der verwalteten Geräte und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

   In der Liste werden nur die verwalteten Geräte der ausgewählten Administrationsgruppe angezeigt.
3. Suchen Sie in der Liste das Gerät, für das Sie Informationen anzeigen möchten, und klicken Sie auf den Gerätenamen.
4. Wechseln Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts zur Registerkarte **Apps**.
5. Klicken Sie in der Liste der auf dem Gerät installierten Kaspersky-Apps auf den Namen der App **Kaspersky Endpoint Security 12.1 für Linux**.

   Das Eigenschaftenfenster der App wird geöffnet.

Im Fenster **Kaspersky Endpoint Security 12.1 für Linux** werden die folgenden Informationen über Kaspersky Endpoint Security angezeigt:

- Die Registerkarte **Allgemein** im Abschnitt **Informationen** enthält allgemeine Informationen zur installierten Anwendung:
  - **Name** – Name der Anwendung.
  - **Versionsnummer** – Versionsnummer der App.
  - **Installiert** – Datum und Uhrzeit der Installation der App auf dem Gerät.
  - **Letztes Software-Update** — Datum und Uhrzeit des letzten Updates der Module von Kaspersky Endpoint Security.
  - **Letzte Synchronisierung** – Datum und Uhrzeit der letzten Verbindung des Geräts mit dem Administrationsserver von Kaspersky Security Center.
  - **Aktueller Status** – Status des Schutzes vor bedrohlichen Dateien, z. B.: *Wird ausgeführt* oder *Angehalten*.
  - Der Block **Installierte Updates** enthält Informationen über Updates für die Module der App.

- Der Block **Anwendungsdatenbank** enthält für die Anwendungsdatenbank Informationen über Datum und Uhrzeit der Veröffentlichung des Updates sowie Datum und Uhrzeit der letzten Aktualisierung.

- Die Registerkarte **Allgemein** im Abschnitt **Lizenzen** enthält Informationen über die der App hinzugefügten Lizenzschlüssel und über die mit diesen Schlüsseln verknüpften Lizenzen.

- Die Registerkarte **Allgemein** im Abschnitt **Komponenten** enthält eine Liste der funktionalen Komponenten der App. Für jede Komponente wird ihr Status (z. B. *Gestoppt, Angehalten, Nicht installiert*) und ihre Version angezeigt.

  In der Zeile **Light Agent-Modus zum Schutz virtueller Umgebungen** können Sie Informationen über die Art der Verwendung der App anzeigen:

  - Der *Ausführungsstatus* gibt an, dass die App im Light Agent-Modus verwendet wird.

  - Der Status *Nicht installiert* gibt an, dass die App im Standard-Modus verwendet wird.

- Auf der Registerkarte **Ereignisse** wird eine Liste mit den Ereignissen der App auf dem Gerät angezeigt.

- Die Registerkarte **Ereigniskonfiguration** zeigt die Arten der Ereignisse, welche die App im Ereignisspeicher speichert, sowie deren Speicherdauer an.

- Auf der Registerkarte **Anwendungseinstellungen** können Sie im Abschnitt **Detection and Response** die Netzwerkisolation des Geräts verwalten.

Informationen über die Ausführung der App in der Verwaltungskonsole anzeigen

So zeigen Sie Informationen über die Ausführung der App in der Verwaltungskonsole von Kaspersky Security Center an:

1. Wählen Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center im Ordner **Verwaltete Geräte** die Administrationsgruppe aus, die das benötigte Gerät enthält.

2. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.

3. Wählen Sie in der Liste der verwalteten Geräte das erforderliche Gerät aus und öffnen Sie das Fenster **Eigenschaften: <Gerätename>** mit einem Doppelklick.

4. Wählen Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts den Abschnitt **Anwendungen** aus.

   Im rechten Teil des Fensters wird eine Liste der auf dem Gerät installierten Apps von Kaspersky angezeigt.

5. Wählen Sie die App **Kaspersky Endpoint Security 12.1 für Linux** aus und öffnen Sie das Fenster mit den App-Eigenschaften, indem Sie doppelklicken oder die Schaltfläche **Eigenschaften** unten im Fenster verwenden.

   Das Fenster **Einstellungen von Kaspersky Endpoint Security 12.1 für Linux** wird geöffnet.

Im Fenster **Einstellungen für Kaspersky Endpoint Security 12.1 für Linux** werden die folgenden Informationen über Kaspersky Endpoint Security angezeigt:

- Im Abschnitt **Allgemein** finden Sie allgemeine Informationen zur installierten App:

  - **Versionsnummer** – Versionsnummer der App.

  - **Installiert** – Datum und Uhrzeit der Installation der App auf dem Gerät.

- **Aktueller Status** – Status des Schutzes vor bedrohlichen Dateien, z. B.: *Wird ausgeführt* oder *Angehalten*.
- **Letztes Software-Update** — Datum und Uhrzeit des letzten Updates der Module von Kaspersky Endpoint Security.
- **Installierte Updates** — Liste der Module, für die Updates installiert wurden.
- **App-Datenbanken** – Datum und Uhrzeit der Veröffentlichung des Datenbanken-Updates der App.

- Der Abschnitt **Komponenten** enthält eine Liste der Standardkomponenten der App. Für jede Komponente wird ihr Status (z. B. *Gestoppt, Angehalten, Nicht installiert*) und ihre Version angezeigt.

  In der Zeile **Light Agent-Modus zum Schutz virtueller Umgebungen** können Sie Informationen über die Art der Verwendung der App anzeigen:

  - Der *Ausführungsstatus* gibt an, dass die App im Light Agent-Modus verwendet wird.
  - Der Status *Nicht installiert* gibt an, dass die App im Standard-Modus verwendet wird.

- Der Abschnitt **Lizenzschlüssel** enthält Informationen zum aktiven Lizenzschlüssel und zum Reserve-Lizenzschlüssel:

  - **Seriennummer** – Eindeutige alphanumerische Zeichenfolge.
  - **Status** – Status des Lizenzschlüssels, z. B. aktiv oder Reserve.
  - **Typ** – Typ der Lizenz: Kommerziell oder Test.
  - Die **Gültigkeitsdauer der Lizenz** ist die Anzahl der Tage, die bis zum Ende der Nutzungsdauer der App verbleiben, welche vorher durch das Hinzufügen dieses Schlüssels aktiviert wurde.
  - **Lizenzbeschränkung** – Anzahl der Geräte, auf denen der Schlüssel verwendet werden kann.
  - **Aktivierungsdatum** (dieses Feld ist nur für den aktiven Schlüssel verfügbar) – Datum des Hinzufügens des aktiven Schlüssels.
  - **Gültigkeitsdauer** (dieses Feld ist nur für den aktiven Schlüssel verfügbar) – Ende der Nutzungsdauer der App, welche durch das Hinzufügen eines aktiven Schlüssels aktiviert wurde.

- Der Abschnitt **Ereigniskonfiguration** zeigt die Arten der Ereignisse, welche die App im Ereignisspeicher speichert, sowie deren Speicherdauer an.
- Der Abschnitt **Erweitert** enthält Informationen zum Verwaltungs-Plug-in für die App.

Informationen über die Ausführung der App über die Befehlszeile anzeigen

Um Informationen zur App anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --app-info [--json]
```

Wobei gilt: `--json` – Gibt Daten im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

- **Name**. Name der App.
- **Version**. Aktuelle Version der App.
- **Richtlinie**. Informationen darüber, ob die Richtlinie von Kaspersky Security Center auf dem Gerät angewendet wird.
- **Informationen über die App-Lizenz** . Informationen über die Lizenz der App oder den Status des Lizenzschlüssels der App.
- **Informationen über die Lizenz von EDR Optimum**. Informationen über die Lizenz, unter der die Funktionalität von Kaspersky Endpoint Detection and Response Optimum genutzt wird, oder Status des Lizenzschlüssels von EDR Optimum.
- **Abonnementstatus**. Status des Abonnements. Dieses Feld wird angezeigt, wenn die App im Rahmen eines Abonnements ausgeführt wird.
- **Gültigkeitsdauer der App-Lizenz**. Datum und Uhrzeit des Ablaufs der App-Lizenz im UTC-Format.
- **Gültigkeitsdauer der Lizenz von EDR Optimum**. Zeitpunkt (Datum und Uhrzeit im UTC-Format), an dem die Lizenz zur Nutzung der Funktionen von Kaspersky Endpoint Detection and Response abläuft.
- **Status der MDR-BLOB-Datei**. Der Status der BLOB-Konfigurationsdatei für die Integration von Kaspersky Managed Detection and Response.
- **Gültigkeitsdauer der Lizenz von MDR-BLOB**. Zeitpunkt (Datum und Uhrzeit im UTC-Format), an dem die Lizenz zur Verwendung von Managed Detection and Response abläuft.
- **Backup-Status**. Status des Backups.
- **Auslastung des Backups**. Größe des Backups.
- **Datum des letzten Starts der Aufgabe Scan_My_Computer**. Der Zeitpunkt, an dem die Aufgabe Schadsoftware-Untersuchung zuletzt ausgeführt wurde.
- **Datum der letzten Veröffentlichung der App-Datenbanken**. Uhrzeit der letzten Veröffentlichung der App-Datenbanken.
- **Geladene App-Datenbanken**. Informationen darüber, ob die App-Datenbanken geladen sind.
- **Verwendung von Kaspersky Security Network**. Informationen zur Verwendung von Kaspersky Security Network: `Erweiterter KSN-Modus`, `Standardmäßiger KSN-Modus` oder `Deaktiviert`.
- **Light Agent-Modus zum Schutz virtueller Umgebungen**. Informationen darüber, dass die App im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird. Wenn die App im Standard-Modus ausgeführt wird, ist diese Zeile ausgeblendet.
- **Desinfektion und Löschen von Dateien ist deaktiviert**. Information, dass jener Ausführungsmodus der App aktiviert ist, in dem die Dateien auf der Festplatte weder desinfiziert noch gelöscht werden, unabhängig von den in den Eigenschaften der Richtlinie eingestellten Parametern.
- **Infrastruktur von Kaspersky Security Network**. Informationen zu der Infrastrukturlösung, die für die Interaktion mit den Reputationsdatenbanken von Kaspersky verwendet wird: `Kaspersky Security Network` oder `Kaspersky Private Security Network`.

- **Integration mit Kaspersky Managed Detection and Response**. Status der Integration mit Kaspersky Managed Detection and Response: `Aktiviert`, `Deaktiviert`.
- **Integration mit Kaspersky Endpoint Detection and Response Optimum** Status der Integration mit Kaspersky Endpoint Detection and Response Optimum.
- **Schutz vor bedrohlichen Dateien**. Status des Schutzes vor bedrohlichen Dateien in Echtzeit.
- **Container-Überwachung**. Status der Untersuchung von Containern in Echtzeit.
- **Überwachung der System-Integrität**. Status der Komponente Überwachung der Systemintegrität.
- **Firewall-Verwaltung**. Status der Komponente Firewall-Verwaltung.
- **Schutz vor Verschlüsselung**. Status der Komponente Schutz vor Verschlüsselung.
- **Schutz vor Web-Bedrohungen**. Status der Komponente Schutz vor Web-Bedrohungen.
- **Gerätekontrolle**. Status der Komponente Gerätekontrolle.
- **Untersuchung von Wechseldatenträgern**. Status der Komponente Untersuchung von Wechseldatenträgern.
- **Schutz vor Netzwerkbedrohungen**. Status der Komponente Schutz vor Netzwerkbedrohungen.
- **Verhaltensanalyse**. Status der Komponente Verhaltensanalyse.
- **App-Kontrolle**. Status der Komponente App-Kontrolle.
- **Web-Kontrolle**. Status der Komponente Web-Kontrolle.
- **Integration mit Kaspersky Endpoint Detection and Response (KATA)**. Status der Integration mit Kaspersky Endpoint Detection and Response (KATA).
- **Aktionen nach dem Update**. Verfügbarkeit von App-Updates und Aktionen, die der Benutzer ausführen muss.
- **App-Ausführung ist instabil**. Zeigt Informationen zum Absturz der App und zum Erstellen einer Dump-Datei an. Dieses Feld wird angezeigt, wenn es beim vorherigen Start der App einen Absturz gab.

App aktivieren und Lizenzschlüssel verwalten

Aktivierung – Vorgang, bei dem die App durch eine Lizenz aktiviert wird, die die Nutzung der Vollversion der App während der Gültigkeitsdauer der Lizenz ermöglicht.

Das Verfahren zur Aktivierung von Kaspersky Endpoint Security umfasst das Hinzufügen des aktiven Lizenzschlüssels der App.

Wenn Sie die App unter einer Lizenz verwenden, welche die Funktionalität von Kaspersky Endpoint Detection and Response Optimum nicht abdeckt, müssen Sie zur Aktivierung dieser Funktionalität einen zusätzlichen Lizenzschlüssel für das Add-on von Kaspersky Endpoint Detection and Response Optimum hinzufügen (im Weiteren auch "EDR Optimum-Schlüssel").

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, ist die separate Aktivierung der App nicht notwendig. Sie aktivieren Kaspersky Security for Virtualization Light Agent und die Aktivierung erfolgt auf der Seite des Schutzservers (dies ist eine Komponente von Kaspersky Security for Virtualization Light Agent) durch das Hinzufügen eines Lizenzschlüssels auf der SVM. Um die Funktionen von Kaspersky Endpoint Detection and Response Optimum zu aktivieren, müssen Sie der SVM auch den EDR Optimum-Schlüssel hinzufügen.

Sie können die App auf eine der folgenden Arten aktivieren:

- Per Fernzugriff über Kaspersky Security Center:
  - Während der Installation von Kaspersky Endpoint Security. Sie können dem Installationspaket einen Lizenzschlüssel hinzufügen. Die App wird nach der Installation automatisch aktiviert.
  - Nach der Installation von Kaspersky Endpoint Security. Sie können der App einen Lizenzschlüssel hinzufügen, indem Sie die Aufgabe zur App-Aktivierung verwenden oder indem Sie einen Lizenzschlüssel, der sich auf dem Administrationsserver befindet, an Client-Geräte verteilen.
- Über die Befehlszeile:
  - Während der Erstkonfiguration von Kaspersky Endpoint Security.
  - Nach der Installation von Kaspersky Endpoint Security. Sie können Lizenzschlüssel mithilfe von Verwaltungsbefehlen hinzufügen und entfernen.

Sie können der App auch einen Reserveschlüssel hinzufügen. Der Reserveschlüssel wird aktiv, sobald die an den aktiven Schlüssel gebundene gültige Lizenz abläuft oder der aktive Schlüssel gelöscht wird. Ein Reserveschlüssel verhindert, dass nach Ablauf der Lizenz die Funktionalität der App eingeschränkt wird.

Ein Reserveschlüssel kann nur hinzugefügt werden, wenn bereits ein aktiver Lizenzschlüssel hinzugefügt wurde.

Sie können Informationen zu den Lizenzschlüsseln, die dem Gerät hinzugefügt wurden, anzeigen:

- Per Fernzugriff in der Web Console oder in der Verwaltungskonsole. In den App-Eigenschaften auf dem Client-Gerät werden im Abschnitt **Lizenzschlüssel** Informationen zum aktiven Schlüssel und zum Reserveschlüssel angezeigt.
- Über die Befehlszeile mithilfe von Verwaltungsbefehlen.

Lizenz- und Schlüsselinformationen über die Befehlszeile anzeigen

Über die Befehlszeile können Sie mit dem Befehl `-L --query` Informationen über den der App hinzugefügten aktiven Lizenzschlüssel und den Reserve-Lizenzschlüssel sowie die Lizenz anzeigen, mit der die App aktiviert wurde. Wenn der App ein separater Schlüssel hinzugefügt wird, um die Funktionalität von Kaspersky Endpoint Detection and Response Optimum zu aktivieren, werden auch die Informationen über die aktiven Schlüssel und Reserveschlüssel von EDR Optimum und über die Lizenz von EDR Optimum angezeigt.

Um Informationen über Lizenzschlüssel und Lizenzen auf einem Gerät anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control -L --query [--json]
```

Wobei gilt: `--json` – Gibt Daten im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

- Informationen über den aktiven App-Schlüssel, sofern ein Schlüssel hinzugefügt wurde:
  - Das Datum und die Uhrzeit des Ablaufs der Gültigkeitsdauer der Lizenz, mit der die App verwendet wird.
  - Die Anzahl der Tage bis zum Ablauf der Gültigkeitsdauer der Lizenz.
  - Informationen zu Einschränkungen der Schutzfunktionen.
  - Informationen zu Einschränkungen der Funktion zum Update der App-Datenbanken.
  - Informationen zum Status des Lizenzschlüssels.
  - Der mit dem Schlüssel verknüpfte Lizenztyp.
  - Beschränkung des Lizenzschlüssels (Anzahl der Lizenzierungseinheiten).
  - Der Name der App, die der Schlüssel aktivieren soll.
  - Aktiver Lizenzschlüssel (eindeutige alphanumerische Zeichenfolge).
  - Datum der Aktivierung.
- Informationen zum aktiven Reserveschlüssel der App Wird angezeigt, wenn die App im Standard-Modus verwendet wird und ein Reserveschlüssel hinzugefügt wurde. Wenn die App im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, werden Informationen zum Reserveschlüssel nicht angezeigt; der Reserveschlüssel wird der SVM hinzugefügt.
  - Das Datum und die Uhrzeit des Ablaufs der Gültigkeitsdauer der Lizenz, mit der die App verwendet wird.
  - Die Anzahl der Tage bis zum Ablauf der Gültigkeitsdauer der Lizenz.
  - Informationen zu Einschränkungen der Schutzfunktionen.
  - Informationen zu Einschränkungen der Funktion zum Update der App-Datenbanken.

- Informationen zum Status des Lizenzschlüssels.
- Der mit dem Schlüssel verknüpfte Lizenztyp.
- Beschränkung des Lizenzschlüssels (Anzahl der Lizenzierungseinheiten).
- Der Name der App, die der Schlüssel aktivieren soll.
- Datum der Aktivierung.

- Informationen über den aktiven EDR Optimum-Schlüssel, sofern ein Schlüssel hinzugefügt wurde:
  - Das Datum und die Uhrzeit des Ablaufs der Gültigkeitsdauer der Lizenz, mit der die Funktionalität von Kaspersky Endpoint Detection and Response Optimum aktiviert wurde.
  - Informationen zu Einschränkungen der Funktion zum Update der App-Datenbanken.
  - Informationen zum Status des Lizenzschlüssels.
  - Der mit dem Schlüssel verknüpfte Lizenztyp.
  - Beschränkung des Lizenzschlüssels (Anzahl der Lizenzierungseinheiten).
  - Der Name der App, die der Schlüssel aktivieren soll.
  - Aktiver Lizenzschlüssel (eindeutige alphanumerische Zeichenfolge).
  - Datum der Aktivierung.
- Informationen zum aktiven Reserveschlüssel von EDR Optimum Wird angezeigt, wenn die App im Standard-Modus verwendet wird und ein Reserveschlüssel für EDR Optimum hinzugefügt wurde. Wenn die App im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, werden Informationen zum Reserveschlüssel nicht angezeigt; der Reserveschlüssel wird der SVM hinzugefügt.
  - Das Datum und die Uhrzeit des Ablaufs der Gültigkeitsdauer der Lizenz, mit der die Funktionalität von Kaspersky Endpoint Detection and Response Optimum aktiviert wurde.
  - Informationen zu Einschränkungen der Funktion zum Update der App-Datenbanken.
  - Informationen zum Status des Lizenzschlüssels.
  - Der mit dem Schlüssel verknüpfte Lizenztyp.
  - Beschränkung des Lizenzschlüssels (Anzahl der Lizenzierungseinheiten).
  - Der Name der App, die der Schlüssel aktivieren soll.
  - Datum der Aktivierung.

Lizenzschlüssel über die Befehlszeile verwalten

Um die Lizenzschlüssel auf einem Gerät zu verwalten, können Sie die Befehle zur Verwaltung von Lizenzschlüsseln verwenden.

Mit diesen Befehlen können Sie sowohl Lizenzschlüssel für die App als auch für EDR Optimum hinzufügen. Der Schlüsseltyp muss nicht im Befehl angeben werden.

Die Befehle zur Verwaltung von Lizenzschlüsseln können nur ausgeführt werden, wenn die App im Standard-Modus verwendet wird. Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, schlagen die Befehle zur Verwaltung von Lizenzschlüsseln mit einem Fehler fehl. Sie aktivieren die App als Teil der Lösung Kaspersky Security for Virtualization Light Agent; Sie müssen die App nicht separat aktivieren.

Um der App einen aktiven Lizenzschlüssel hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control [-L] --add-active-key <Pfad der Schlüsseldatei / Aktivierungscode>
```

Wobei gilt:

- `Pfad der Schlüsseldatei` – Pfad der Schlüsseldatei. Wenn sich die Schlüsseldatei im aktuellen Verzeichnis befindet, ist die Angabe des Dateinamens ausreichend.
- `Aktivierungscode` – Aktivierungscode.

Um der App einen Reserve-Lizenzschlüssel hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control [-L] --add-reserve-key <Pfad der Schlüsseldatei / Aktivierungscode>
```

Wenn der App auf dem Gerät noch kein aktiver Schlüssel hinzugefügt wurde, schlägt der Befehl fehl.

Um den aktiven App-Schlüssel zu entfernen, führen Sie den folgenden Befehl aus:

```
kesl-control [-L] --remove-active-key
```

Um den Reserveschlüssel der App zu entfernen, führen Sie den folgenden Befehl aus:

```
kesl-control [-L] --remove-reserve-key
```

Um den aktiven EDR Optimum-Schlüssel zu entfernen, führen Sie den folgenden Befehl aus:

```
kesl-control [-L] --remove-active-key --edr-optimum
```

Um den Reserveschlüssel für EDR Optimum zu entfernen, führen Sie den folgenden Befehl aus:

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

Datenbanken und Module der App aktualisieren

Ein Update der Datenbanken und Module von Kaspersky Endpoint Security gewährleistet, dass der Schutz des Geräts auf dem neuesten Stand ist. Weltweit tauchen praktisch täglich neue Viren, Schadsoftware und andere Programme auf, die eine Bedrohung darstellen. Die Datenbanken der App enthalten Informationen über Bedrohungen und Möglichkeiten für deren Neutralisierung. Um Bedrohungen rasch erkennen zu können, müssen Sie die Datenbanken und Module der App regelmäßig aktualisieren.

Für regelmäßige Datenbanken-Updates ist eine aktuelle Lizenz zur Nutzung der App erforderlich. Wenn Sie über keine gültige Lizenz verfügen, können Sie nur ein Mal ein Update durchführen.

Während des Update-Vorgangs werden Datenbanken und Module der App heruntergeladen und auf Ihrem Gerät installiert.

Sie können Updates für die Datenbanken und Module der App von den Update-Servern von Kaspersky, aus der Datenverwaltung des Administrationsservers, aus lokalen oder Netzwerkverzeichnissen und von anderen Update-Quellen erhalten.

Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, wird das Verzeichnis auf der SVM als Update-Quelle verwendet.

Während des Updates werden die Module und die Datenbanken der App auf Ihrem Gerät mit der aktuellen Version in der Update-Quelle verglichen. Wenn Ihre aktuellen Datenbanken und Module der App von den jeweiligen neuesten Versionen abweichen, wird der fehlende Teil der Updates auf Ihrem Gerät installiert.

Wenn die Datenbanken stark veraltet sind, kann das Update-Paket groß sein, was zu zusätzlichem Internet-Datenverkehr (bis zu mehreren MB) führen kann. Der Umfang des erforderlichen Speicherplatzes kann bis zu 3 GB betragen.

Die Updates werden von Kaspersky-Update-Servern oder von anderen FTP-, HTTP- oder HTTPS-Servern über Standard-Netzwerkprotokolle heruntergeladen. Standardmäßig werden die Internetverbindungseinstellungen automatisch bestimmt. Wenn Sie einen Proxy-Server verwenden, geben Sie die Proxy-Server-Einstellungen in den allgemeinen App-Einstellungen an.

Unabhängig von der Update-Quelle erfolgt das Herunterladen des Update-Pakets und die Installation von Updates für die Datenbanken und Module der App auf dem Gerät mithilfe der Aufgabe *Update*.

Die App erstellt eine vordefinierte Aufgabe vom Typ *Update*. Mit dieser Aufgabe können Sie die Datenbanken und Module der App nach einem Zeitplan und auf Befehl aktualisieren und Update-Einstellungen konfigurieren.

Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, werden die Datenbanken auf geschützten virtuellen Maschinen mithilfe einer speziellen und lokalen Aufgabe *Update* aktualisiert, bei welcher als Update-Quelle ein Verzeichnis auf der SVM angegeben wurde. Diese Update-Aufgabe wird automatisch gestartet. Sie können diese Aufgabe weder löschen noch ihre Einstellungen ändern.

Das Aktualisieren von Datenbanken und Modulen der App mithilfe von Aufgaben, die in Kaspersky Security Center erstellt wurden, wird nicht unterstützt.

Wenn Kaspersky Endpoint Security im Standard-Modus verwendet wird, können Sie in Kaspersky Security Center die Gruppenaufgabe *Update* verwenden, die der Assistent für die Ersteinrichtung nach der Installation des MMC-Plug-ins oder des Web-Plug-ins für die Verwaltung von Kaspersky Endpoint Security erstellt.

Sie können Benutzeraufgaben für Updates auch über die Befehlszeile und in Kaspersky Security Center erstellen.

Sie können die folgenden Einstellungen für die Aktualisierung der Datenbanken und Module der App konfigurieren:

- Wählen Sie je nach verwendetem Update-Szenario die Quelle aus, aus der die App die Updates erhalten soll.
- Konfigurieren Sie die Wartezeit auf eine Antwort von der ausgewählten Update-Quelle beim Versuch, eine Verbindung herzustellen. Wenn in der angegebenen Zeit keine Antwort von der Update-Quelle eingeht, greift die App auf eine andere angegebene Update-Quelle zu.
- Wählen Sie den Modus zum Herunterladen und Installieren der Module und Update-Versionen der App: "Herunterladen und installieren", "Nur herunterladen" oder "Nicht herunterladen".
- Konfigurieren Sie den Zeitplan für den Start der Update-Aufgabe. Standardmäßig aktualisiert die App die Datenbanken einmal alle 60 Minuten.

Informationen zum Aktualisieren von Datenbanken und Modulen

Während der Durchführung eines Updates werden die folgenden Objekte heruntergeladen und auf Ihrem Gerät installiert:

- App-Datenbanken. Zu den App-Datenbanken gehören Datenbanken mit Signaturen von Schadsoftware, Beschreibungen von Netzwerkangriffen, Datenbanken mit bösartigen Webadressen und Phishing-Adressen, Datenbanken mit Bannern, Spam-Datenbanken und andere Daten.

  Wenn die Aktualisierung der Datenbanken auf dem Gerät unterbrochen wird oder mit einem Fehler fehlschlägt, verwendet die App weiterhin die zuvor installierte Version der Datenbanken. Wenn bisher noch keine App-Datenbanken installiert wurden, wird die App im Modus "ohne Datenbanken" ausgeführt. Die Aktualisierung der Datenbanken und Module der App ist weiterhin verfügbar.

  Datenbanken sind aktuell, wenn sie vor weniger als drei Tagen heruntergeladen wurden. Standardmäßig generiert die App das Ereignis *Datenbanken veraltet* (*BasesAreOutOfDate*), wenn die neuesten installierten Datenbank-Updates vor mehr als drei, aber weniger als sieben Tagen auf den Servern von Kaspersky veröffentlicht wurden. Wenn die Datenbanken nicht innerhalb von sieben Tagen aktualisiert werden, generiert die App das Ereignis *Datenbanken stark veraltet* (*BasesAreTotallyOutOfDate*).

- App-Module. Modul-Updates dienen dazu, Schwachstellen in der App zu beseitigen und die Schutztechniken für das Gerät zu verbessern. Modul-Updates können das Verhalten von App-Komponenten anpassen und neue Funktionen hinzufügen.

  Ein Update der App kann unabhängig vom Status der App (gestartet, gestoppt, durch eine Richtlinie von Kaspersky Security Center verwaltet) und dem Update-Zeitplan installiert werden. Während eines Updates der App-Module setzt Kaspersky Endpoint Security den Schutz Ihres Gerätes fort. Während eines Updates werden die Einstellungen der App und das Ereignisprotokoll der App auf die neue App-Version übertragen. Starten Sie Kaspersky Endpoint Security nach der Aktualisierung neu.

  Wenn die Übertragung der Einstellungen aus irgendeinem Grund fehlschlägt, wird die App auf die Standardwerte zurückgesetzt.

  Änderungen an den App-Einstellungen, die Sie nach Abschluss der Aktualisierung und vor dem Neustart der App vornehmen, werden nicht gespeichert.

  Nach einem Update der App-Version mittels Autopatch ändert sich der Mechanismus zur Interaktion mit der Firewall des Betriebssystems: Die Regeln werden mit den System-Tools "iptables" und "iptables-restore" verwaltet.

Wenn die App nach einem Update nicht ordnungsgemäß funktioniert, wird sie automatisch auf die vorherige Version zurückgesetzt. Es wird empfohlen, Kontakt mit dem Technischen Support von Kaspersky aufzunehmen.

Informationen zu Update-Quellen und -Szenarien

Update-Quelle – Eine Ressource, die Datenbanken-Updates und Updates der Module der App Kaspersky Endpoint Security enthält. Als Update-Quelle können FTP-, HTTP- oder HTTPS-Server (z. B. die Update-Server von Kaspersky) sowie lokale Verzeichnisse und Netzwerkverzeichnisse dienen, die von den Benutzern gemountet sind.

Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, werden Datenbanken auf geschützten virtuellen Maschinen aus dem Verzeichnis auf der SVM aktualisiert.

Als primäre Update-Quelle dienen die Kaspersky-Update-Server. Sie können andere Update-Quellen in den Einstellungen der Aufgabe *Update* angeben. Wenn ein Update aus einer bestimmten Update-Quelle nicht durchgeführt werden kann, verbindet sich Kaspersky Endpoint Security mit der nächsten Quelle.

Die App Kaspersky Endpoint Security unterstützt die folgenden Szenarien für das Update von Datenbanken und Modulen:

- Update von den Kaspersky-Update-Servern Die Kaspersky-Update-Server befinden sich in verschiedenen Ländern auf der ganzen Welt, was eine hohe Zuverlässigkeit der Updates gewährleistet. Wenn ein Update von einem bestimmten Server aus nicht durchgeführt werden kann, wechselt die App zum nächsten Server. Die Updates werden über das HTTPS-Protokoll heruntergeladen.

- Zentralisiertes Update Das zentralisierte Update reduziert den externen Internetverkehr und ermöglicht eine bequeme Überwachung des Updates.

  Das zentralisierte Update besteht aus den folgenden Schritten:

  1. Laden Sie das Update-Paket in einen Speicher im Unternehmensnetzwerk herunter.

     Als Speicher können Sie die Datenverwaltung des Administrationsservers von Kaspersky Security Center verwenden.

     Das Update-Paket wird von der Aufgabe des Administrationsservers *Download von Updates in die Datenverwaltung des Administrationsservers* in die Datenverwaltung des Administrationsservers heruntergeladen.

     Wenn Sie die App mit der Kaspersky Security Center Cloud Console verwalten, können Sie den Speicher von Verteilungspunkten (Geräte, auf denen der Administrationsagent installiert ist) als Speicher verwenden. Nähere Informationen über Verteilungspunkte finden Sie in der Hilfe zu Kaspersky Security Center.

  2. Verteilen Sie das Update-Paket an die Client-Geräte.

     Das Update-Paket wird von der *Update*-Aufgabe der App Kaspersky Endpoint Security an die Client-Geräte verteilt. In den Aufgabeneinstellungen müssen Sie den Administrationsserver von Kaspersky Security Center als Update-Quelle auswählen.

- Aktualisierung aus einem lokalen Verzeichnis oder Netzwerkverzeichnis (SMB/NFS), das vom Benutzer gemountet wurde, oder von einem FTP-, HTTP- oder HTTPS-Server. Sie können eine benutzerdefinierte Update-Quelle in den Einstellungen der Aufgabe *Update* angeben.

Datenbanken und Module der App in der Web Console aktualisieren

Das Verfahren zur Aktualisierung der Datenbanken und Module von Kaspersky Endpoint Security hängt vom Nutzungsmodus der App ab. In diesem Abschnitt wird beschrieben, wie Sie die App im Standard-Modus aktualisieren. Wenn Sie die App im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, wird das Aktualisieren von Datenbanken und Modulen der App mithilfe von in Kaspersky Security Center erstellten Aufgaben nicht unterstützt. Das Update wird über einen lokale vordefinierte Aufgabe durchgeführt.

In der Web Console können Sie die Datenbanken und Module der App mithilfe der Aufgabe *Update* aktualisieren. Sie können die automatisch erstellte Gruppenaufgabe *Update* verwenden und auch Benutzeraufgaben für Updates erstellen.

So konfigurieren Sie Update-Einstellungen in der Web Console:

1. Wählen Sie im Hauptfenster der Web Console die Option **Assets (Geräte)** → **Aufgaben**.

   Die Liste mit Aufgaben wird geöffnet.

2. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf allen Geräten einer bestimmten Administrationsgruppe ausgeführt wird, klicken Sie auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

     In der Liste werden nur die Aufgaben angezeigt, die für die ausgewählte Administrationsgruppe konfiguriert sind.

   - Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf einem oder mehreren Geräten ausgeführt wird (Aufgaben für eine Gerätegruppe), klicken Sie auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster den oberen Knoten mit dem Namen des Administrationsservers.

     In der Liste werden alle auf dem Administrationsserver erstellten Aufgaben angezeigt.

3. Wählen Sie in der Aufgabenliste die erforderliche **Update**-Aufgabe aus und öffnen Sie über den Link im Aufgabennamen das Fenster mit den Aufgabeneigenschaften.

4. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **App-Einstellungen** und in der Liste links den Abschnitt **Update-Quellen** aus.

5. Wählen Sie je nach verwendetem Update-Szenario die Update-Quelle aus, aus der die App je nach Update-Schema die Updates für die Datenbanken und Modul bezieht.

   Wenn Sie die App über Web Console verwalten, enthält die Liste der Update-Quellen die Kaspersky-Update-Server und den Administrationsserver von Kaspersky Security Center. Wenn Sie die App über die Kaspersky Security Center Cloud Console verwalten, enthält die Liste der Update-Quellen die Kaspersky-Update-Server und Verteilungspunkte (weitere Informationen zu Verteilungspunkten finden Sie in der Hilfe zu Kaspersky Security Center). Sie können der Liste weitere Update-Quellen hinzufügen.

   Sie können eine Liste der Update-Quellen erstellen, indem Sie die Option **Andere Quellen im lokalen oder globalen Netzwerk** auswählen. Sie können FTP-, HTTP- oder HTTPS-Server als Update-Quellen angeben. Wenn ein Update aus einer bestimmten Update-Quelle nicht durchgeführt werden kann, verbindet sich Kaspersky Endpoint Security mit der nächsten Quelle. Die App wendet sich der Reihe nach so an die Update-Quellen, wie sie in der Tabelle platziert wurden.

6. Gehen Sie zum Abschnitt **Einstellungen** und konfigurieren Sie die weiteren Update-Einstellungen.

7. Wählen Sie die Registerkarte **Zeitplan** aus und konfigurieren Sie den Zeitplan für den Start der Update-Aufgabe.

Wenn Sie **Kaspersky Security Center** als Update-Quelle ausgewählt haben, wählen Sie in der Dropdown-Liste **Geplanter Start** die Option **Wenn Updates in den Speicher heruntergeladen werden** aus. Nähere Informationen über Aufgabenzeitpläne finden Sie in der Hilfe zu Kaspersky Security Center.

8. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die Aufgabe wird gemäß dem konfigurierten Zeitplan gestartet. Sie können die Aufgabe auch manuell starten.

Abschnitt "Update-Quellen für die Update-Aufgabe"

Einstellung	Beschreibung
Update-Quellen	In diesem Block können Sie die Update-Quelle auswählen: • **Kaspersky-Update-Server**, auf denen Datenbanken-Updates für alle Apps von Kaspersky veröffentlicht werden (Standardwert). • **Kaspersky Security Center** – Kaspersky Security Center Administrationsserver (nur für die Web Console verfügbar). • **Verteilungspunkte** (nur für Kaspersky Security Center Cloud Console verfügbar). • **Andere Quellen im lokalen oder globalen Netzwerk** – HTTP-, HTTPS- oder FTP-Server bzw. Verzeichnisse auf Servern im lokalen Netzwerk.
Kaspersky-Update-Server verwenden, wenn keine anderen Update-Quellen verfügbar sind	Dieses Kontrollkästchen aktiviert und deaktiviert die Verwendung der Kaspersky-Update-Server als Update-Quellen, wenn die angegebenen Update-Quellen nicht verfügbar sind. Dieses Kontrollkästchen ist verfügbar, wenn im Block **Update-Quellen** die Variante **Andere Quellen im lokalen oder globalen Netzwerk** oder die Option **Administrationsserver von Kaspersky Security Center** ausgewählt ist. Das Kontrollkästchen ist standardmäßig aktiviert.
Benutzerdefinierte Update-Quellen	Diese Tabelle enthält eine Liste mit benutzerdefinierten Quellen für Datenbanken-Updates. Während des Updates wendet sich die App der Reihe nach so an die Update-Quellen, wie sie in der Tabelle platziert wurden. Folgende Spalten sind in der Tabelle enthalten: • **Update-Quelle** – HTTP-, HTTPS- oder FTP-Server oder Verzeichnisse auf Servern des lokalen Netzwerks. • Der Schalter zeigt an, ob die Quelle in einer Aufgabe verwendet wird (**Aktiviert** bzw. **Deaktiviert**). Sie können den Schalter in der Tabelle aktivieren oder deaktivieren. Darüber hinaus können Sie das Kontrollkästchen **Diese Quelle verwenden** im Fenster **Update-Quelle**, das über den Link mit dem Namen der Quelle geöffnet wird, aktivieren oder deaktivieren. Diese Tabelle ist verfügbar, wenn die Variante **Andere Quellen im lokalen oder globalen Netzwerk** ausgewählt ist. Standardmäßig die Tabelle leer. Sie können Update-Quellen in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben. Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Abschnitt "Einstellungen der Update-Aufgabe"

Einstellung	Beschreibung
Maximale Wartezeit auf eine Antwort der Update-Quelle (Sek.)	Maximale Wartezeit (in Sekunden), der App auf eine Antwort von der ausgewählten Update-Quelle. Wenn bis zu diesem Zeitpunkt keine Antwort eingeht, wird im Protokoll der Aufgabenausführung ein Ereignis mit dem Hinweis auf den Verlust der Verbindung zur Update-Quelle gespeichert. Zulässige Werte: 0 – 120. Ist der Wert "0" angegeben, dann ist die Wartezeit für eine Antwort auf die Anfrage der App von der ausgewählten Quelle nicht beschränkt. Standardwert: 10 Sekunden
Download-Modus für App-Updates	In dieser Dropdown-Liste können Sie Download-Modus für die App-Updates festlegen: • Updates **nicht herunterladen**. Wenn diese Option ausgewählt ist, kann die App nicht aktualisiert werden. • Updates **nur herunterladen**, ohne sie auf den Client-Geräten zu installieren (Standardwert). • **Herunterladen und installieren** der Updates auf Client-Geräten Nach der Installation der Updates wird die App automatisch neu gestartet. Diese Funktionalität wird im KESL-Container nicht unterstützt.

Datenbanken und Module der App in der Verwaltungskonsole aktualisieren

Das Verfahren zur Aktualisierung der Datenbanken und Module von Kaspersky Endpoint Security hängt vom Nutzungsmodus der App ab. In diesem Abschnitt wird beschrieben, wie Sie die App im Standard-Modus aktualisieren. Wenn Sie die App im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, wird das Aktualisieren von Datenbanken und Modulen der App mithilfe von in Kaspersky Security Center erstellten Aufgaben nicht unterstützt. Das Update wird über einen lokale vordefinierte Aufgabe durchgeführt.

In der Verwaltungskonsole können Sie die Datenbanken und Module der App mithilfe der Aufgabe *Update* aktualisieren. Sie können die automatisch erstellte Gruppenaufgabe *Update* verwenden und auch Benutzeraufgaben für Updates erstellen.

So konfigurieren Sie Update-Einstellungen in der Verwaltungskonsole:

1. Führen Sie in der Verwaltungskonsole eine der folgenden Aktionen aus:

   - Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf Geräten ausgeführt wird, die zu einer bestimmten Administrationsgruppe gehören, wählen Sie diese Administrationsgruppe in der Konsolenstruktur aus und wählen Sie dann im Arbeitsbereich die Registerkarte **Aufgaben** aus.

   - Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf einem oder mehreren Geräten ausgeführt wird (Aufgaben für eine Gerätegruppe), wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.

2. Wählen Sie in der Aufgabenliste die erforderliche **Update**-Aufgabe aus und öffnen Sie das Eigenschaftenfenster der Aufgabe mit einem Doppelklick.

3. Wählen Sie im Eigenschaftenfenster der Aufgabe in der Liste links den Abschnitt **Update-Quellen** aus.

4. Wählen Sie je nach verwendetem Update-Szenario die Update-Quelle aus, aus der die App je nach Update-Schema die Updates für die Datenbanken und Modul bezieht.

   Die Liste mit Update-Quellen enthält die Kaspersky-Update-Server und den Administrationsserver von Kaspersky Security Center. Sie können der Liste weitere Update-Quellen hinzufügen.

   Sie können eine Liste der Update-Quellen erstellen, indem Sie die Option **Andere Quellen im lokalen oder globalen Netzwerk** auswählen. Sie können FTP-, HTTP- oder HTTPS-Server als Update-Quellen angeben. Wenn ein Update aus einer bestimmten Quelle nicht durchgeführt werden kann, verbindet sich Kaspersky Endpoint Security mit der nächsten Quelle. Die App wendet sich der Reihe nach so an die Update-Quellen, wie sie in der Tabelle platziert wurden.

5. Wählen Sie den Abschnitt **Einstellungen** aus und konfigurieren Sie die weiteren Update-Einstellungen.

6. Wählen Sie den Abschnitt **Zeitplan** aus und konfigurieren Sie den Zeitplan für den Start der Update-Aufgabe.

   Wenn Sie **Kaspersky Security Center** als Update-Quelle ausgewählt haben, wählen Sie in der Dropdown-Liste **Geplanter Start** die Option **Wenn Updates in den Speicher heruntergeladen werden** aus. Nähere Informationen über Aufgabenzeitpläne finden Sie in der Hilfe zu Kaspersky Security Center.

7. Klicken Sie im Fenster **Eigenschaften: <Aufgabenname>** auf die Schaltfläche **Übernehmen** oder die Schaltfläche **OK**, um die Änderungen zu speichern.

Die Aufgabe wird gemäß dem konfigurierten Zeitplan gestartet. Sie können die Aufgabe auch manuell starten.

Abschnitt "Update-Quellen für die Update-Aufgabe"

Einstellung	Beschreibung
Update-Quellen	In diesem Block können Sie die Update-Quelle auswählen: • **Kaspersky-Update-Server**, auf denen Datenbanken-Updates für alle Apps von Kaspersky veröffentlicht werden (Standardwert).

	• **Kaspersky Security Center** – Kaspersky Security Center Administrationsserver. • **Andere Quellen im lokalen oder globalen Netzwerk** – HTTP-, HTTPS- oder FTP-Server bzw. Verzeichnisse auf Servern im lokalen Netzwerk.
Kaspersky-Update-Server verwenden, wenn keine anderen Update-Quellen verfügbar sind	Dieses Kontrollkästchen aktiviert und deaktiviert die Verwendung der Kaspersky-Update-Server als Update-Quellen, wenn die angegebenen Update-Quellen nicht verfügbar sind. Dieses Kontrollkästchen ist verfügbar, wenn im Block **Update-Quellen** die Variante **Andere Quellen im lokalen oder globalen Netzwerk** oder die Option **Administrationsserver von Kaspersky Security Center** ausgewählt ist. Das Kontrollkästchen ist standardmäßig aktiviert.
Benutzerdefinierte Update-Quellen	Diese Tabelle enthält eine Liste mit benutzerdefinierten Quellen für Datenbanken-Updates. Während des Updates wendet sich die App der Reihe nach so an die Update-Quellen, wie sie in der Tabelle platziert wurden. Folgende Spalten sind in der Tabelle enthalten: • **Adresse der Quelle** – Enthält die HTTP-, HTTPS- oder FTP-Server oder Verzeichnisse auf den Servern des lokalen Netzwerks. • **Status** zeigt an, ob die Quelle in einer Aufgabe verwendet wird (**Wird verwendet** bzw. **Wird nicht verwendet**). Sie können den Status ändern, indem Sie das Kontrollkästchen **Diese Quelle verwenden** im Fenster **Update-Quelle** aktivieren oder deaktivieren. Dieses Fenster wird geöffnet, wenn Sie auf die Schaltfläche **Bearbeiten** klicken. Diese Tabelle ist verfügbar, wenn die Variante **Andere Quellen im lokalen oder globalen Netzwerk** ausgewählt ist. Sie können Update-Quellen in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben. Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

	Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können. Standardmäßig die Tabelle leer.

Abschnitt "Einstellungen der Update-Aufgabe"

Einstellung	Beschreibung
Maximale Wartezeit auf eine Antwort der Update-Quelle (Sek.)	Maximale Wartezeit (in Sekunden), der App auf eine Antwort von der ausgewählten Update-Quelle. Wenn bis zu diesem Zeitpunkt keine Antwort eingeht, wird im Protokoll der Aufgabenausführung ein Ereignis mit dem Hinweis auf den Verlust der Verbindung zur Update-Quelle gespeichert. Zulässige Werte: 0 – 120. Ist der Wert "0" angegeben, dann ist die Wartezeit für eine Antwort auf die Anfrage der App von der ausgewählten Quelle nicht beschränkt. Standardwert: 10 Sekunden
Download-Modus für Updates	In dieser Dropdown-Liste können Sie Download-Modus für die App-Updates festlegen: • Updates **nicht herunterladen**. Wenn diese Option ausgewählt ist, kann die App nicht aktualisiert werden. • Updates **nur herunterladen**, ohne sie auf den Client-Geräten zu installieren (Standardwert). • **Herunterladen und installieren** der Updates auf Client-Geräten Nach der Installation der Updates wird die App automatisch neu gestartet. Diese Funktionalität wird im KESL-Container nicht unterstützt.

Datenbanken und Module der App über die Befehlszeile aktualisieren

Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, werden die Datenbanken auf geschützten virtuellen Maschinen mithilfe einer speziellen und lokalen Aufgabe *Update* aktualisiert, bei welcher als Update-Quelle ein Verzeichnis auf der SVM angegeben wurde. Diese Update-Aufgabe wird automatisch gestartet. Sie können diese Aufgabe weder löschen noch ihre Einstellungen ändern.

In der Befehlszeile können Sie die Datenbanken und Module der App auf folgende Arten aktualisieren:

- Mithilfe der vordefinierten Update-Aufgabe (*Update*). Sie können diese Aufgabe manuell starten, beenden, anhalten und fortsetzen und den Zeitplan für den Aufgabenstart konfigurieren. Sie können Untersuchungseinstellungen konfigurieren, indem Sie die Einstellungen für diese Aufgabe ändern.
- Mithilfe von Benutzeraufgaben für Updates (Aufgaben vom Typ *Update*). Sie können Benutzeraufgaben manuell starten und den Zeitplan für den Aufgabenstart konfigurieren.

Einstellungen der Update-Aufgabe

Einstellung	Beschreibung	Werte

`SourceType`	Quelle, aus der die App die Updates erhalten soll.	`KLServers` (Standardwert) – Die App ruft Updates von einem der Kaspersky-Update-Server ab. Die Updates werden über das HTTPS-Protokoll heruntergeladen. `SCServer` – Die App lädt die Updates von einem im lokalen Netzwerk installierten Administrationsserver auf das geschützte Gerät herunter. Sie können diese Updatequelle auswählen, wenn Sie Kaspersky Security Center für die zentrale Verwaltung des Schutzes der Geräte in Ihren Unternehmen benutzen. `Custom` – Die App lädt Updates von der im Abschnitt `[CustomSources.item_#]` angegebenen benutzerdefinierten Quelle herunter. Sie können Verzeichnisse auf FTP-, HTTP-, und HTTPS-Servern und Verzeichnisse auf einem beliebigen gemounteten Gerät des geschützten Client-Geräts angeben, einschließlich der Verzeichnisse auf Remote-Geräten, die über Samba- oder NFS-Protokolle gemountet sind.
`UseKLServersWhenUnavailable`	Die App kontaktiert die Kaspersky-Update-Server, falls keine der benutzerdefinierten Quellen verfügbar ist.	`Yes` (Standardwert) – Die App greift auf Kaspersky-Update-Server zu, wenn keine benutzerdefinierten Update-Quellen verfügbar sind. `No` – Die App greift nicht auf Kaspersky-Update-Server zu, wenn keine benutzerdefinierten Update-Quellen verfügbar sind.
`ApplicationUpdateMode`	Modus für den Download und die Installation der App-Updates.	`Disabled` – Keine App-Updates herunterladen und installieren. `DownloadOnly` (Standardwert) – App-Updates herunterladen, aber nicht installieren. `DownloadAndInstall` – App-Updates automatisch herunterladen und installieren. Nach der Installation der Updates wird die App automatisch neu gestartet.
`ConnectionTimeout`	Wartezeit (in Sekunden) auf eine Antwort von der Update-Quelle beim Versuch, eine Verbindung herzustellen. Wenn im angegebenen Zeitraum keine Antwort von der Update-Quelle eingeht, greift die App auf eine andere angegebene Update-Quelle zu.	Sie können nur ganze Zahlen zwischen 0 und 120 angeben. Standardwert: 10.

Der Abschnitt **[CustomSources.item_#]** enthält die folgenden Einstellungen:		
`URL`	Adresse der benutzerdefinierten Update-Quelle im lokalen Netzwerk oder im Internet.	Der Standardwert ist nicht angegeben. Beispiele: `URL=http://example.com/bases/` – Adresse des HTTP-Servers, auf dem sich das Verzeichnis mit den Updates befindet. `URL=/home/bases/` – Verzeichnis mit den App-Datenbanken auf dem geschützten Gerät.
`Enabled`	Verwendung der in der Einstellung `URL` angegebenen Update-Quelle. Um die Aufgabe abzuschließen, müssen Sie mindestens eine Update-Quelle aktivieren.	`Yes` – Die App verwendet die Update-Quelle. `No` – Die App verwendet Updatequelle nicht. Der Standardwert ist nicht angegeben.

Update mithilfe von Kaspersky Update Utility

Um den Internetverkehr zu reduzieren, können Sie auf den Geräten im lokalen Unternehmensnetzwerk das Update von Datenbanken und Modulen der App aus einem freigegebenen Verzeichnis mithilfe von Kaspersky Update Utility einrichten. Zu diesem Zweck muss eines der Geräte im lokalen Unternehmensnetzwerk Update-Pakete vom Administrationsserver von Kaspersky Security Center oder von den Kaspersky-Update-Servern empfangen und die empfangenen Update-Pakete anschließend mithilfe des Tools in das freigegebene Verzeichnis kopieren. Andere Geräte im lokalen Unternehmensnetzwerk können das Update-Paket aus dem freigegebenen Verzeichnis abrufen.

So konfigurieren Sie das Update der Datenbanken aus dem freigegebenen Verzeichnis mithilfe von Kaspersky Update Utility:

1. Installieren Sie Kaspersky Update Utility auf einem Gerät im lokalen Unternehmensnetzwerk.

   Sie können das Programmpaket von Kaspersky Update Utility von der Website des Technischen Supports von Kaspersky herunterladen.

2. Konfigurieren Sie das Kopieren des Update-Pakets in das freigegebene Verzeichnis in den Einstellungen von Kaspersky Update Utility.

   Wählen Sie die Update-Quelle (z. B. die Datenverwaltung des Administrationsservers) und das freigegebene Verzeichnis aus, in die Kaspersky Update Utility die Update-Pakete kopieren soll. Nähere Informationen zur Verwendung von Kaspersky Update Utility finden Sie in der Kaspersky-Wissensdatenbank.

3. Konfigurieren Sie die Updates der Datenbanken und Module der App aus dem angegebenen freigegebenen Verzeichnis auf den übrigen Geräten im lokalen Unternehmensnetzwerk.

a. Öffnen Sie die Eigenschaften der Aufgabe **Update**, die auf dem erforderlichen Gerät ausgeführt werden soll, über Web Console oder über die Verwaltungskonsole.

b. Wechseln Sie in den Aufgabeneigenschaften zum Abschnitt **Update-Quellen**.

c. Wählen Sie im Block **Update-Quellen** die Option **Andere Quellen im lokalen oder globalen Netzwerk** aus.

4. Klicken Sie in der Tabelle der Update-Quellen auf die Schaltfläche **Hinzufügen** und geben Sie den Pfad zum freigegebenen Verzeichnis an.

   Die Adresse der Quelle muss mit der in den Einstellungen von Kaspersky Update Utility angegebenen Adresse übereinstimmen.

5. Aktivieren Sie das Kontrollkästchen **Diese Quelle verwenden** und klicken Sie auf **OK**.

6. Legen Sie in der Tabelle der Update-Quellen mit den Schaltflächen **Nach oben** und **Nach unten** die Reihenfolge fest, in der sie verwendet werden.

7. Speichern Sie die Änderungen an den Aufgabeneinstellungen.

Update der Datenbanken und Module der App zurücksetzen

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, wird das Rollback des Datenbanken-Updates mittels einer Aufgabe nicht unterstützt.

Nach dem erstmaligen Update der App-Datenbanken wird die Rollback-Funktion verfügbar, mit der die App-Datenbanken auf eine frühere Version zurückgesetzt werden können.

Jedes Mal, wenn der Benutzer den Update-Vorgang startet, erstellt die App Kaspersky Endpoint Security eine Backup-Kopie der aktuellen App-Datenbanken. Auf diese Weise können Sie bei Bedarf die Datenbanken auf eine frühere Version zurücksetzen.

Das Rollback des letzten Datenbanken-Updates ist z. B. dann sinnvoll, wenn die neue Version der App-Datenbanken eine ungültige Signatur enthält, weswegen die App Kaspersky Endpoint Security eine sichere App blockiert.

In der Befehlszeile zum Rollback von Updates können Sie die vordefinierte Rollback-Datenbankaktualisierungsaufgabe (Rollback) *ausführen* oder benutzerdefinierte Update-Rollback-Aufgaben (Rollback -Aufgaben) *erstellen* und ausführen.

In Kaspersky Security Center können Sie über Web Console oder über die Verwaltungskonsole Update-Rollback-Aufgaben für Administrationsgruppen oder einzelne Geräte erstellen.

Die Aufgabe *Rollback des Datenbanken-Updates* hat keine Einstellungen.

Schutz vor bedrohlichen Dateien

Die Komponente "Schutz vor bedrohlichen Dateien" verhindert eine Infektion des Dateisystem des Geräts. Die Komponente wird beim Start von Kaspersky Endpoint Security automatisch mit den Standardeinstellungen aktiviert, befindet sich dauerhaft im Arbeitsspeicher des Geräts und untersucht in Echtzeit alle Dateien, die geöffnet, gespeichert und ausgeführt werden.

Wenn Schadsoftware entdeckt wird, kann Kaspersky Endpoint Security die infizierte Datei löschen und den von dieser Datei gestarteten schädlichen Prozess beenden.

Der Modus des Moduls zum Abfangen von Dateioperationen, den Sie in den allgemeinen App-Einstellungen auswählen können, wirkt sich auf die Ausführung der Komponente aus. Während der Untersuchung wird der Zugriff auf eine Datei standardmäßig blockiert.

Wenn der Schutz vor bedrohlichen Dateien und die Container-Überwachung aktiviert sind, scannt die App auch alle Namespaces und Container auf allen unterstützten Betriebssystemen.

Sie können den Schutz vor bedrohlichen Dateien ein- und ausschalten und auch Schutzeinstellungen konfigurieren:

- Wählen Sie den Modus für die Untersuchung von Dateien aus (beim Öffnen, beim Öffnen und Ändern).
- Aktivieren und deaktivieren Sie die Untersuchung von Archiven, E-Mail-Datenbanken und E-Mail-Nachrichten im Textformat.
- Schließen Sie Dateien im Textformat vorübergehend aus der erneuten Untersuchung aus.
- Begrenzen Sie die Größe des untersuchten Objekts und die Untersuchungsdauer für das Objekt.
- Wählen Sie die Aktionen aus, welche die App für infizierte Objekte ausführen soll.
- Schränken Sie den Untersuchungsbereich ein. Die App untersucht Objekte im angegebenen Bereich des Dateisystems.
- Konfigurieren Sie den Ausschluss von Objekten aus der Untersuchung. *Ausschluss von der Untersuchung* – Eine Reihe von Bedingungen, die erfüllt sein müssen, damit die App Objekte nicht auf Viren und andere Schadsoftware überprüft. Sie können Folgendes von der Untersuchung ausschließen:
  - Objekte nach Namen oder Masken;
  - Objekte nach dem Namen der in den Objekten gefundenen Bedrohungen;
  - Dateien und Verzeichnisse in bestimmten Bereichen des Dateisystems;
  - Prozesse und Dateien, die durch den angegebenen Prozess geändert wurden.
- Konfigurieren Sie die Verwendung der heuristischen Analyse und der iChecker-Technologie während der Untersuchung.
- Aktivieren und deaktivieren Sie die Protokollierung von Informationen zu untersuchten nicht infizierten Objekten, zu untersuchten Objekten in Archiven und zu nicht verarbeiteten Objekten.

Um die Ausführung der Komponente zum Schutz vor bedrohlichen Dateien zu optimieren, können Sie den Ausschluss von Dateien, die aus Netzwerkverzeichnissen kopiert wurden, von der Untersuchung konfigurieren. Dateien werden erst untersucht, nachdem das Kopieren in das lokale Verzeichnis abgeschlossen ist. Um Dateien in Netzwerkverzeichnissen von der Untersuchung auszuschließen, müssen Sie für ein Tool, das zum Kopieren aus Netzwerkverzeichnissen bestimmt ist (z. B. für das Tool `cp`) einen Ausschluss nach Prozess konfigurieren. Wenn Sie die App mithilfe von Kaspersky Security Center verwalten, können Sie den Ausschluss nach Prozess in der Web Console oder in der Verwaltungskonsole konfigurieren. Wenn Sie die App über die Befehlszeile verwalten, können Sie den Ausschluss nach Prozess konfigurieren, indem Sie den Abschnitt [ExcludedForProgram.item_#] zu den `Einstellungen für OAS-Aufgaben hinzufügen`.

Schutz vor bedrohlichen Dateien in der Web Console konfigurieren

In der Web Console können Sie den Schutz vor bedrohlichen Dateien in den Eigenschaften einer Richtlinie verwalten (**App-Einstellungen** → **Basisschutz** → **Schutz vor bedrohlichen Dateien**).

Einstellungen der Komponente zum Schutz vor bedrohlichen Dateien

Einstellung	Beschreibung
Schutz vor bedrohlichen Dateien aktiviert/deaktiviert	Dieser Schalter aktiviert und deaktiviert die Komponente zum Schutz vor bedrohlichen Dateien auf allen verwalteten Geräten. Der Schalter ist standardmäßig aktiviert.
Modus für den Schutz vor bedrohlichen Dateien	In dieser Dropdown-Liste können Sie den Modus für die Ausführung der Komponente zum Schutz vor bedrohlichen Dateien auswählen: • **Intelligenter Modus** (Standardwert) – Die Datei wird bei versuchter Öffnung und erneut bei versuchtem Schließen untersucht, falls die Datei verändert wurde. Wenn ein Prozess während seiner Ausführung mehrmals auf eine Datei zugreift und diese verändert, wird diese Datei erst dann erneut untersucht, wenn der Prozess die Datei das letzte Mal schließt. • **Beim Öffnen** – Untersucht eine Datei bei versuchtem Zugriff zum Lesen, Ausführen oder Bearbeiten. • **Beim Öffnen und Ändern** – Untersucht eine Datei bei versuchtem Öffnen und erneut bei versuchtem Schließen, falls die Datei verändert wurde.
Erste Aktion	In der Dropdown-Liste können Sie die erste Aktion auswählen, die von der App für das gefundene infizierte Objekt ausgeführt werden soll: • Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Informationen zur Gefahrenstufe der in der Datei erkannten Bedrohung und zur Möglichkeit ihrer Desinfektion (Standardwert). • Zugriff auf das Objekt **blockieren**.
Zweite Aktion	In dieser Dropdown-Liste können Sie die zweite Aktion auswählen, die von der App für ein infiziertes Objekt ausgeführt werden soll, falls die erste Aktion nicht erfolgreich war:

	• Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Daten zur in der Datei erkannten Gefahrenstufe der Bedrohung und zur Möglichkeit ihrer Desinfektion. • Zugriff auf das Objekt **blockieren** (Standardwert).
Untersuchungsbereiche	Der Link **Untersuchungsbereiche anpassen** öffnet das Fenster **Schutzbereiche**.
Archive untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Archiven. Wenn das Kontrollkästchen aktiviert ist, so untersucht die App Archive. Um ein Archiv zu untersuchen, muss es zunächst von der App entpackt werden, was die Untersuchung verlangsamen kann. Sie können die Dauer der Untersuchung von Archiven reduzieren, indem Sie die Einstellungen **Dateien überspringen, deren Untersuchung länger dauert als (Sek.)** und/oder **Dateien überspringen, die größer sind als (MB)** aktivieren und konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Archive. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Selbstentpackende Archive untersuchen	Das Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung *selbstentpackender Archive (self-extracting archives)*. Selbstentpackende Archive sind Archive, die ein ausführbares Modul zum Entpacken enthalten. Wenn das Kontrollkästchen aktiviert ist, untersucht die App selbstentpackende Archive. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine selbstentpackenden Dateien. Dieses Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Archive untersuchen** deaktiviert ist. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Mail-Datenbanken untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Mail-Datenbanken der Anwendungen Microsoft Outlook, Outlook Express, The Bat! und anderen E-Mail-Clients. Wenn das Kontrollkästchen aktiviert ist, untersucht die App die Dateien von Mail-Datenbanken. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Dateien von Mail-Datenbanken. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Dateien in Mail-Formaten untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Dateien von E-Mail-Nachrichten im Textformat (plain text). Wenn das Kontrollkästchen aktiviert ist, untersucht die App E-Mail-Nachrichten im Textformat. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App E-Mail-Nachrichten im Textformat nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Textdateien überspringen	Dateien im Textformat vorübergehend von der Untersuchung ausschließen.

	Wenn das Kontrollkästchen aktiviert ist, untersucht die App keine Dateien im Textformat, wenn diese Dateien innerhalb von 10 Minuten nach der letzten Untersuchung von demselben Prozess wiederverwendet werden. Mit diesem Parameter können Sie die Untersuchung von Protokollen zur Ausführung der App optimieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App Textdateien. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Dateien überspringen, deren Untersuchung länger dauert als (Sek.)	In diesem Feld können Sie die erlaubte Höchstdauer für die Untersuchung der Datei in Sekunden angeben. Nach Ablauf des angegebenen Zeitraums bricht die App die Untersuchung der Datei ab. Zulässige Werte: `0–9999`. Ist der Wert `0` angegeben, dann ist die Untersuchungsdauer nicht beschränkt. Der Standardwert ist `60`.
Dateien überspringen, die größer sind als (MB)	In diesem Feld können Sie die maximale Größe der untersuchten Datei in Megabyte angeben. Zulässige Werte: `0–999999`. Ist der Wert `0` angegeben, untersucht die App Dateien jeder Größe. Der Standardwert ist `0`.
Virenfreie Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung des Ereignisses *ObjectProcessed*. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App das Ereignis *ObjectProcessed* für jedes untersuchte Objekt. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App das Ereignis nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Unverarbeitete Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung des Ereignisses *ObjectNotProcessed*, wenn eine Datei während der Untersuchung nicht verarbeitet werden kann. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App das Ereignis *ObjectNotProcessed*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App das Ereignis nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Gepackte Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung des Ereignisses *PackedObjectDetected* für alle erkannten gepackten Objekte. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App das Ereignis *PackedObjectDetected*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App das Ereignis nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
iChecker-Technologie verwenden	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung nur neuer oder seit der letzten Untersuchung geänderter Dateien. Wenn das Kontrollkästchen aktiviert ist, untersucht die App nur neue oder seit der letzten Untersuchung geänderte Dateien. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App Dateien unabhängig von ihrem Erstellungs- oder Änderungsdatum. Das Kontrollkästchen ist standardmäßig aktiviert.
Heuristische Analyse	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die heuristische Analyse bei

verwenden	der Untersuchung von Objekten. Das Kontrollkästchen ist standardmäßig aktiviert.
Stufe der heuristischen Analyse	Wenn das Kontrollkästchen **Heuristische Analyse verwenden** aktiviert ist, können Sie die Ebene der heuristischen Analyse in der Dropdown-Liste festlegen: • **Oberflächlich** – Die am wenigsten detaillierte Untersuchung, minimale Systembelastung. • **Mittel** – Mittlere Untersuchung, ausgeglichene Systembelastung. • **Tief** – Detaillierteste Untersuchung, maximale Systembelastung. • **Empfohlen** (Standardwert) – Optimale Stufe, die von den Kaspersky-Experten empfohlen wird. Sie bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Server.

Fenster "Schutzbereiche"

Die Tabelle enthält den Untersuchungsbereich. Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle einen Schutzbereich, der alle Verzeichnisse des lokalen Dateisystems umfasst.

Einstellungen des Schutzbereichs

Einstellung	Beschreibung
Name des Bereichs	Name des Untersuchungsbereichs
Pfad	Der Pfad zu dem zu untersuchenden Verzeichnis.
Status	Der Status gibt an, ob die App diesen Bereich während ihrer Ausführung untersucht.

Sie können Elemente in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.

Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Liste der Bereiche angeben sind. Um bei Bedarf für das Unterverzeichnis andere Sicherheitseinstellungen festzulegen als für das übergeordnete Verzeichnis, platzieren Sie erforderlichenfalls das Unterverzeichnis in der Liste über dem übergeordneten Verzeichnis.

Fenster zum Hinzufügen des Schutzbereichs

In diesem Fenster können Sie einen neuen Schutzbereich hinzufügen oder anpassen.

Einstellungen des Schutzbereichs

Einstellung	Beschreibung
Name des Bereichs	Eingabefeld für den Namen des Schutzbereichs. Dieser Name wird in der Tabelle im Fenster **Untersuchungsbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung dieses Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, verarbeitet die App diesen Schutzbereich während der Ausführung. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die App diesen Schutzbereich während der Ausführung nicht. Sie können diesen Bereich zu einem späteren Zeitpunkt zu den Betriebseinstellungen der Komponente hinzufügen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	In der Dropdown-Liste können Sie den Typ des Dateisystems auswählen: • **Lokal** (Standardwert) – Lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie den Pfad zu einem lokalen Verzeichnis angeben.

	• **Mounted** – Gemountete Remote-Verzeichnisse oder lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie das Protokoll oder den Namen des Dateisystems angeben. • **Freigegeben** – Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind. • **Alle freigegebenen** – Alle Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind.
Zugriffsprotokoll	In der Dropdown-Liste können Sie das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind. Diese Dropdown-Liste ist verfügbar, wenn in der Dropdown-Liste für Dateisysteme als Typ **Freigegeben** oder **Mounted** ausgewählt ist.
Pfad	Eingabefeld für den Pfad des Verzeichnisses, das in den Schutzbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken und Tags verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

	Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardmäßige Pfadangabe **/** – Die App untersucht alle Verzeichnisse des lokalen Dateisystems. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Lokal** ausgewählt ist. Wenn in der Dropdown-Liste der Dateisysteme als Typ **Lokal** ausgewählt ist und kein Pfad angegeben wird, untersucht die App alle Verzeichnisse des lokalen Dateisystems.
Name der freigegebenen Ressource	Eingabefeld für den Namen der freigegebenen Ressource des Dateisystems, auf der sich die Verzeichnisse befinden, die Sie zum Schutzbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste **Zugriffsprotokoll** das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der App während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster. Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Ausschlüsse aus dem Schutz vor bedrohlichen Dateien

Ein *Ausschluss aus dem Schutz* ist eine Reihe von Bedingungen, die erfüllt sein müssen, damit die App Kaspersky Endpoint Security Objekte nicht auf Viren und andere Schadsoftware überprüft. Sie können Objekte auch anhand des Namens oder des maskierten Namens der Bedrohung aus dem Schutz ausschließen und Ausschlüsse für Prozesse konfigurieren.

In der Web Console können Sie die Ausnahmen für den Schutz vor bedrohlichen Dateien in den Eigenschaften der Richtlinie konfigurieren (**App-Einstellungen** → **Basisschutz** → **Ausnahmen des Schutzes vor bedrohlichen Dateien**).

Einstellungen der Ausschlüsse aus dem Schutz

Einstellung	Beschreibung
Ausschlussbereiche	Der Link **Ausschlussbereiche anpassen** öffnet das Fenster **Ausschlussbereiche**. In diesem Fenster können Sie eine Liste mit Ausschlüssen aus dem Schutz festlegen.
Ausschlüsse nach Maske	Der Link **Ausschlüsse nach Maske anpassen** öffnet das Fenster **Ausschlüsse nach Maske**. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren.
Ausschlüsse nach Bedrohungsname	Der Link **Ausschlüsse nach Bedrohungsname anpassen** öffnet das Fenster **Ausschlüsse nach Bedrohungsname**. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren.
Ausschlüsse nach Prozess	Der Link **Ausschlüsse nach Prozessen anpassen** öffnet das Fenster **Ausschlüsse nach Prozessen**. In diesem Fenster können Sie den Ausschluss der Aktivität von Prozessen aus der Untersuchung konfigurieren.

Fenster "Ausschlussbereiche"

Die Tabelle enthält Bereiche mit Ausschlüsse von der Untersuchung. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der App angewendet wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster zum Hinzufügen des Ausschlussbereichs

In diesem Fenster können Sie einen neuen Ausschlussbereich hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster **Ausschlussbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss des Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, wird dieser Bereich während der Ausführung der App von der Untersuchung oder vom Schutz ausgeschlossen. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich während der Ausführung der App in die Untersuchung oder den Schutz eingeschlossen. Im Folgenden können Sie diesen Bereich von der Untersuchung oder dem Schutz ausschließen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	In der Dropdown-Liste können Sie den Typ des Dateisystems auswählen, auf dem sich die Verzeichnisse befinden, die Sie zu den Ausschlüssen von der Untersuchung hinzufügen möchten: • **Lokal** – Lokale Verzeichnisse. • **Mounted** – Remote-Verzeichnisse, die auf dem Gerät eingebunden sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind.
Zugriffsprotokoll	In der Dropdown-Liste können Sie das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind. Diese Dropdown-Liste ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** ausgewählt ist.
Pfad	Eingabefeld für den Pfad des Verzeichnisses, das in den Ausschlussbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken und Tags

verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

	Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Als Pfad ist standardmäßig **/** angegeben: Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Lokal** ausgewählt ist.
Name der freigegebenen Ressource	Eingabefeld für den Namen der freigegebenen Ressource des Dateisystems, auf der sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten: Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste **Zugriffsprotokoll** das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Untersuchung ausgeschlossen werden. Die Masken werden nur innerhalb des Verzeichnisses übernommen, das im Eingabefeld **Pfad** angegeben ist. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen. Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist. Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Maske"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren. Die App untersucht keine Dateien, deren Namen die angegebenen Masken enthalten. Standardmäßig ist die Liste mit Masken leer.

Sie können Masken hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist.

Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Bedrohungsname"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren. Die App blockiert die angegebenen Bedrohungen nicht. Standardmäßig ist die Liste mit den Namen von Bedrohungen leer.

Sie können Namen von Bedrohungen hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Bedrohung aus den Ausschlüsse.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens ein Bedrohungsname ausgewählt ist.

Ein Klick auf den Namen einer Bedrohung in der Tabelle öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung ändern, die von der Untersuchung ausgenommen wird.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung angeben, die von der Untersuchung ausgenommen wird.

Fenster "Ausschlüsse nach Prozess"

Die Tabelle enthält Ausschlussbereiche nach Prozessen. Mit dem Ausschlussbereich nach Prozessen können die Aktivität eines angegebenen Prozesses und die von ihm geänderten Dateien von der Prüfung ausgeschlossen werden. Standardmäßig enthält die Tabelle zwei Ausschlussbereiche, welche die Pfade zu Administrationsagenten enthält. Bei Bedarf können Sie diesen Ausschluss entfernen.

Einstellungen des Ausschlussbereichs nach Prozessen

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Vollständiger Pfad des auszuschließenden Prozesses.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der App angewendet wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Fenster "Vertrauenswürdiger Prozess"

In diesem Fenster können Sie einen Ausschlussbereich nach Prozessen hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs nach Prozess	Eingabefeld für den Namen des Ausschlussbereichs nach Prozessen. Dieser Name wird in der Tabelle im Fenster **Ausschlüsse nach Prozessen** angezeigt. Das Eingabefeld darf nicht leer sein.

Diese Ausschlüsse verwenden bzw. nicht verwenden	Dieser Schalter aktiviert oder deaktiviert den Ausschluss dieses Bereichs während der Ausführung der App. Der Schalter ist standardmäßig aktiviert.
Auf untergeordnete Prozesse anwenden	Untergeordnete Prozesse des Prozesses, der durch den Parameter **Pfad des auszuschließenden Prozesses** ausgeschlossen ist, ebenfalls von der Untersuchung ausschließen. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Pfad des auszuschließenden Prozesses	Vollständiger Pfad des Prozesses, den Sie von der Untersuchung ausschließen möchten.
Dateisystem, Zugriffsprotokoll und Pfad	Diese Einstellungsgruppe erlaubt, Ausschlüsse von der Untersuchung für Dateien festzulegen, die der Prozess verändert. In der Dropdown-Liste der Dateisysteme können Sie den Typ des Dateisystems auswählen, auf dem sich die Verzeichnisse befinden, die von der Untersuchung ausgeschlossen werden sollen: • **Lokal** – Lokale Verzeichnisse. • **Mounted** – Eingebundene Verzeichnisse. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind.
Zugriffsprotokoll	In der Dropdown-Liste können Sie das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind. Die Dropdown-Liste **Zugriffsprotokoll** ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** ausgewählt ist.
Pfad	In diesem Eingabefeld können Sie den Pfad des Verzeichnisses angeben, das in den Ausschlussbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken verwenden.

	Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Lokal** ausgewählt ist.
Name der freigegebenen Ressource	Eingabefeld für den Namen der freigegebenen Ressource des Dateisystems, auf der sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten: Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste **Zugriffsprotokoll** das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Untersuchung ausgeschlossen werden. Masken werden nur innerhalb des Verzeichnisses angewendet, das im Block **Dateisystem, Zugriffsprotokoll und Pfad** angegeben ist. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen. Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist. Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Schutz vor bedrohlichen Dateien in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie den Schutz vor bedrohlichen Dateien in den Eigenschaften einer Richtlinie verwalten (**Basisschutz → Schutz vor bedrohlichen Dateien**).

Einstellungen der Komponente zum Schutz vor bedrohlichen Dateien

Einstellung	Beschreibung
Schutz vor bedrohlichen Dateien aktivieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Komponente zum Schutz vor bedrohlichen Dateien auf allen verwalteten Geräten. Das Kontrollkästchen ist standardmäßig aktiviert.
Modus für den Schutz vor bedrohlichen Dateien	In dieser Dropdown-Liste können Sie den Modus für die Ausführung der Komponente zum Schutz vor bedrohlichen Dateien auswählen: • **Intelligenter Modus** (Standardwert) – Die Datei wird bei versuchter Öffnung und erneut bei versuchtem Schließen untersucht, falls die Datei verändert wurde. Wenn ein Prozess während seiner Ausführung mehrmals auf eine Datei zugreift und diese verändert, wird diese Datei erst dann erneut untersucht, wenn der Prozess die Datei das letzte Mal schließt. • **Beim Öffnen** – Untersucht eine Datei bei versuchtem Zugriff zum Lesen, Ausführen oder Bearbeiten. • **Beim Öffnen und Ändern** – Untersucht eine Datei bei versuchtem Öffnen und erneut bei versuchtem Schließen, falls die Datei verändert wurde.
Untersuchung	Diese Einstellungsgruppe enthält Schaltflächen, mit denen Fenster geöffnet werden können, in denen Sie die Untersuchungsbereiche und die Untersuchungseinstellungen anpassen können.
Aktion beim Erkennen einer Bedrohung	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, mit der das Fenster Aktionen beim Erkennen von Bedrohungen geöffnet werden kann. In diesem Fenster können Sie die Aktionen konfigurieren, die von der App für das erkannte infizierte Objekt ausgeführt werden soll.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält den Untersuchungsbereich. Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle einen Untersuchungsbereich, der alle Verzeichnisse des lokalen Dateisystems umfasst.

Einstellungen des Untersuchungsbereichs

Einstellung	Beschreibung
Name des Bereichs	Name des Untersuchungsbereichs
Pfad	Der Pfad zu dem zu untersuchenden Verzeichnis.
Status	Der Status gibt an, ob die App diesen Bereich während ihrer Ausführung untersucht.

Sie können Elemente in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.

Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Liste der Bereiche angeben sind. Um bei Bedarf für das Unterverzeichnis andere Sicherheitseinstellungen festzulegen als für das übergeordnete Verzeichnis, platzieren Sie erforderlichenfalls das Unterverzeichnis in der Liste über dem übergeordneten Verzeichnis.

Fenster "<Neuer Untersuchungsbereich>"

In diesem Fenster können Sie einen neuen Untersuchungsbereich hinzufügen oder anpassen.

Einstellungen des Untersuchungsbereichs

Einstellung	Beschreibung
Name des Untersuchungsbereichs	Eingabefeld für den Namen der Untersuchungsbereichs. Dieser Name wird in der Tabelle im Fenster **Untersuchungsbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung dieses Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, verarbeitet die App diesen Untersuchungsbereich während ihrer Ausführung. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die App diesen Untersuchungsbereich während ihrer Ausführung nicht. Sie können diesen Bereich zu einem späteren Zeitpunkt zu den Betriebseinstellungen der Komponente hinzufügen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Diese Einstellungsgruppe ermöglicht die Konfiguration des Untersuchungsbereichs. In der Dropdown-Liste der Dateisysteme können Sie den Typ des Dateisystems auswählen: • **Lokal** (Standardwert) – Lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie den Pfad zu einem lokalen Verzeichnis angeben. • **Mounted** – Gemountete Remote-Verzeichnisse oder lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie das Protokoll oder den Namen des Dateisystems angeben. • **Freigegeben** – Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind. • **Alle freigegebenen** – Alle Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind.
	Wenn in der Drop-down-Liste der Dateisysteme der Typ **Alle** oder **Mounted** ausgewählt ist, können Sie rechts in der Drop-down-Liste das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind.
	Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Untersuchungsbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie Masken und Tags verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

	Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardmäßige Pfadangabe **/** – Die App untersucht alle Verzeichnisse des lokalen Dateisystems. Wenn in der Dropdown-Liste der Dateisysteme als Typ **Lokal** ausgewählt ist und kein Pfad angegeben wird, untersucht die App alle Verzeichnisse des lokalen Dateisystems.
Name des Dateisystems	Eingabefeld für den Namen des Dateisystems, auf dem sich die Verzeichnisse befinden, die Sie zum Untersuchungsbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste auf der rechten Seite das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der App während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske ***** (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster. Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Untersuchungseinstellungen"

In diesem Fenster können Sie die Einstellungen für die Untersuchung von Dateien durch den Schutz vor bedrohlichen Dateien konfigurieren.

Einstellungen für den Schutz vor bedrohlichen Dateien

Einstellung	Beschreibung
Archive untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Archiven. Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security Archive. Um ein Archiv zu untersuchen, muss es zunächst von der App entpackt werden, was die Untersuchung verlangsamen kann. Sie können die Dauer der Untersuchung von Archiven reduzieren, indem Sie im Abschnitt **Allgemeine Untersuchungseinstellungen** die Einstellungen **Dateien überspringen, deren Untersuchung länger dauert als (Sek.)** und/oder **Dateien überspringen, die größer sind als (MB)** aktivieren und konfigurieren. Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security Archive nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Selbstentpackende Archive untersuchen	Das Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung *selbstentpackender Archive (self-extracting archives)*. Selbstentpackende Archive sind Archive, die ein ausführbares Modul zum Entpacken enthalten. Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security selbstentpackende Archive. Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security selbstentpackende Archive nicht. Dieses Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Archive untersuchen** deaktiviert ist. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Mail-Datenbanken untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Mail-Datenbanken der Anwendungen Microsoft Outlook, Outlook Express, The Bat! und anderen E-Mail-Clients. Wenn das Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security die Dateien der Mail-Datenbanken. Wenn das Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security die Dateien der Mail-Datenbanken nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Dateien in Mail-Formaten untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Dateien von E-Mail-Nachrichten im Textformat (plain text). Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security E-Mail-Nachrichten im Textformat. Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security E-Mail-Nachrichten im Textformat nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Textdateien überspringen	Dateien im Textformat vorübergehend von der Untersuchung ausschließen.

	Wenn das Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security keine Dateien im Textformat, wenn diese Dateien innerhalb von 10 Minuten nach der letzten Untersuchung von demselben Prozess wiederverwendet werden. Mit diesem Parameter können Sie die Untersuchung von Protokollen zur Ausführung der App optimieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security Textdateien. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Dateien überspringen, deren Untersuchung länger dauert als (Sek.)	In diesem Feld können Sie die erlaubte Höchstdauer für die Untersuchung der Datei in Sekunden angeben. Wenn der angegebenen Zeitpunkt erreicht ist, bricht Kaspersky Endpoint Security die Untersuchung der Datei ab. Zulässige Werte: 0–9999. Ist der Wert 0 angegeben, dann ist die Untersuchungsdauer nicht beschränkt. Standardwert: 60.
Dateien überspringen, die größer sind als (MB)	In diesem Feld können Sie die maximale Größe der untersuchten Datei in Megabyte angeben. Zulässige Werte: 0–999999. Ist der Wert 0 angegeben, untersucht Kaspersky Endpoint Security Dateien jeder Größe. Standardwert: 0.
Virenfreie Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectProcessed*. Wenn dieses Kontrollkästchen aktiviert ist, protokolliert Kaspersky Endpoint Security Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Wenn das Kontrollkästchen deaktiviert ist, protokolliert Kaspersky Endpoint Security keine Ereignisse vom Typ *ObjectProcessed*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Unverarbeitete Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectNotProcessed*, wenn eine Datei während der Untersuchung nicht verarbeitet werden kann. Wenn dieses Kontrollkästchen aktiviert ist, protokolliert Kaspersky Endpoint Security Ereignisse vom Typ *ObjectNotProcessed*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert Kaspersky Endpoint Security keine Ereignisse vom Typ *ObjectNotProcessed*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Gepackte Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *PackedObjectDetected* für alle erkannten gepackten Objekte. Wenn dieses Kontrollkästchen aktiviert ist, protokolliert Kaspersky Endpoint Security Ereignisse vom Typ *PackedObjectDetected*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert Kaspersky Endpoint Security keine Ereignisse vom Typ *PackedObjectDetected*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
iChecker-Technologie verwenden	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung nur neuer oder seit der letzten Untersuchung geänderter Dateien. Wenn das Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security nur neue oder seit der letzten Untersuchung geänderte Dateien. Wenn das Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security Dateien unabhängig von ihrem Erstellungs- oder Änderungsdatum. Das Kontrollkästchen ist standardmäßig aktiviert.

Heuristische Analyse verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die heuristische Analyse bei der Untersuchung von Dateien. Das Kontrollkästchen ist standardmäßig aktiviert.
Stufe der heuristischen Analyse	Wenn das Kontrollkästchen **Heuristische Analyse verwenden** aktiviert ist, können Sie die Ebene der heuristischen Analyse in der Dropdown-Liste festlegen: • **Oberflächlich** – Die am wenigsten detaillierte Untersuchung, minimale Systembelastung. • **Mittel** – Mittlere Untersuchung, ausgeglichene Systembelastung. • **Tief** – Detaillierteste Untersuchung, maximale Systembelastung. • **Empfohlen** (Standardwert) – Optimale Stufe, die von den Kaspersky-Experten empfohlen wird. Sie bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Geräte.

Fenster "Aktion beim Fund einer Bedrohung"

In diesem Fenster können Sie Aktionen auswählen, die von der App Kaspersky Endpoint Security für gefundene infizierte Objekte ausgeführt werden soll.

Einstellungen für den Schutz vor bedrohlichen Dateien

Einstellung	Beschreibung
Erste Aktion	In der Dropdown-Liste können Sie die erste Aktion auswählen, die von der App für das gefundene infizierte Objekt ausgeführt werden soll: • Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Informationen zur Gefahrenstufe der in der Datei erkannten Bedrohung und zur Möglichkeit ihrer Desinfektion (Standardwert). • Zugriff auf das Objekt **blockieren**.
Zweite Aktion	In dieser Dropdown-Liste können Sie die zweite Aktion auswählen, die von der App für ein infiziertes Objekt ausgeführt werden soll, falls die erste Aktion nicht erfolgreich war: • Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Daten zur in der Datei erkannten Gefahrenstufe der Bedrohung und zur Möglichkeit ihrer Desinfektion. • Zugriff auf das Objekt **blockieren** (Standardwert).

Ausschlüsse aus dem Schutz vor bedrohlichen Dateien

Ein *Ausschluss aus dem Schutz* ist eine Reihe von Bedingungen, die erfüllt sein müssen, damit die App Kaspersky Endpoint Security Objekte nicht auf Viren und andere Schadsoftware überprüft. Sie können Objekte auch anhand des Namens oder des maskierten Namens der Bedrohung aus dem Schutz ausschließen und Ausschlüsse für Prozesse konfigurieren.

In der Verwaltungskonsole können Sie die Ausnahmen für den Schutz vor bedrohlichen Dateien in den Eigenschaften der Richtlinie konfigurieren (**Basisschutz → Ausnahmen des Schutzes vor bedrohlichen Dateien**).

Einstellungen der Ausschlüsse von der Untersuchung

Einstellungsgruppe	Beschreibung
Ausschlüsse	Diese Parametergruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausschlussbereiche** öffnet. In diesem Fenster können Sie eine Liste mit Bereichen festlegen, die von der Untersuchung ausgeschlossen werden sollen.
Ausschlüsse nach Maske	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausschlüsse nach Maske** öffnet. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren.
Ausschlüsse nach Bedrohungsname	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausschlüsse nach Bedrohungsname** öffnet. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren.
Ausschlüsse nach Prozess	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausschlüsse nach Prozess** öffnet. In diesem Fenster können Sie den Ausschluss der Aktivität von Prozessen aus der Untersuchung konfigurieren.

Fenster "Ausschlussbereiche"

Die Tabelle enthält Bereiche mit Ausschlüsse von der Untersuchung. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der App angewendet wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "<Neuer Ausschlussbereich>"

In diesem Fenster können Sie einen neuen Bereich mit Untersuchungsausschlüssen hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster **Ausschlussbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss des Bereichs von der Untersuchung während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während ihrer Ausführung von der Untersuchung aus. Wenn das Kontrollkästchen deaktiviert ist, schließt die App diesen Bereich während ihrer Ausführung in die Untersuchung ein. Sie können diesen Bereich zu einem späteren Zeitpunkt ausschließen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Diese Einstellungsgruppe erlaubt die Konfiguration des Ausschlussbereichs. In der Dropdown-Liste der Dateisysteme können Sie den Typ des Dateisystems auswählen, auf dem sich die Verzeichnisse befinden, die von der Untersuchung ausgeschlossen werden sollen: • **Lokal** – Lokale Verzeichnisse. • **Mounted** – Eingebundene Verzeichnisse. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind.
	Wenn in der Drop-down-Liste der Dateisysteme der Typ **Mounted** ausgewählt ist, können Sie rechts in der Drop-down-Liste das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind.
	Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können

Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Ausschlussbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie Masken und Tags verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

	Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Als Pfad ist standardmäßig **/** angegeben: Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus.
Name des Dateisystems	Eingabefeld für den Namen des Dateisystems, auf dem sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste auf der rechten Seite das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Untersuchung ausgeschlossen werden. Die Masken werden nur auf Objekte innerhalb des Verzeichnisses angewendet, das im Eingabefeld des Pfades angegeben ist. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen. Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist. Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Maske"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren. Die App untersucht keine Dateien, deren Namen die angegebenen Masken enthalten. Standardmäßig ist die Liste mit Masken leer.

Sie können Masken hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist.

Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Bedrohungsname"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren. Die App blockiert die angegebenen Bedrohungen nicht. Standardmäßig ist die Liste mit den Namen von Bedrohungen leer.

Sie können Namen von Bedrohungen hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Bedrohung aus den Ausschlüsse.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens ein Bedrohungsname ausgewählt ist.

Ein Klick auf den Namen einer Bedrohung in der Tabelle öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung ändern, die von der Untersuchung ausgenommen wird.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung angeben, die von der Untersuchung ausgenommen wird.

Fenster "Ausschlüsse nach Prozess"

Die Tabelle enthält Ausschlussbereiche nach Prozessen. Mit dem Ausschlussbereich nach Prozessen können die Aktivität eines angegebenen Prozesses und die von ihm geänderten Dateien von der Prüfung ausgeschlossen werden. Standardmäßig enthält die Tabelle zwei Ausschlussbereiche, welche die Pfade zu Administrationsagenten enthält. Bei Bedarf können Sie diesen Ausschluss entfernen.

Einstellungen des Ausschlussbereichs nach Prozessen

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Vollständiger Pfad des auszuschließenden Prozesses.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der App angewendet wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Sie können auch eine Liste von Ausnahmen aus einer Datei importieren, indem Sie auf die Schaltfläche **Erweitert** -> **Importieren** klicken und die Liste der hinzugefügten Ausnahmen über die Schaltflächen **Erweitert** -> **Ausgewählte exportieren** oder **Erweitert** -> **Alle exportieren** in eine Datei exportieren.

Fenster "Vertrauenswürdiger Prozess"

In diesem Fenster können Sie einen Ausschlussbereich nach Prozessen hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs nach Prozessen

Einstellung	Beschreibung
Name des	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle

Ausschlussbereichs	im Fenster **Ausschlüsse nach Prozessen** angezeigt. Das Eingabefeld darf nicht leer sein.
Pfad des auszuschließenden Prozesses	Vollständiger Pfad des Prozesses, den Sie von der Untersuchung ausschließen möchten.
Auf untergeordnete Prozesse anwenden	Untergeordnete Prozesse des Prozesses, der durch den Parameter **Pfad des auszuschließenden Prozesses** ausgeschlossen ist, ebenfalls von der Untersuchung ausschließen. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss dieses Bereichs von der Untersuchung während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während ihrer Ausführung von der Untersuchung aus. Wenn das Kontrollkästchen deaktiviert ist, schließt die App diesen Bereich während ihrer Ausführung in die Untersuchung ein. Sie können diesen Bereich zu einem späteren Zeitpunkt ausschließen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Pfad zu den geänderten Dateien	Diese Einstellungsgruppe erlaubt, Ausschlüsse von der Untersuchung für Dateien festzulegen, die der Prozess verändert. In der Dropdown-Liste der Dateisysteme können Sie den Typ des Dateisystems auswählen, auf dem sich die Verzeichnisse befinden, die von der Untersuchung ausgeschlossen werden sollen: • **Lokal** – Lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie den Pfad zu einem lokalen Verzeichnis angeben. • **Mounted** – Gemountete Remote-Verzeichnisse oder lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie das Protokoll oder den Namen des Dateisystems angeben. • **Freigegeben** – Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind. • **Alle freigegebenen** – Alle Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind.
	Wenn in der Dropdown-Liste der Dateisysteme **Mounted** oder **Alle** ausgewählt ist, können Sie in der Dropdown-Liste der Zugriffsprotokolle das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind.
	Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können

	Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Ausschlussbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie Masken verwenden. Das Eingabefeld darf nicht leer sein. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.
Name des Dateisystems	Eingabefeld für den Namen des Dateisystems, auf dem sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste auf der rechten Seite das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Untersuchung ausgeschlossen werden. Die Masken werden nur innerhalb des Verzeichnisses übernommen, das im Block **Pfad zu den geänderten Dateien** angegeben ist. Sie können Masken hinzufügen, bearbeiten und löschen. Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen. Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist. Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Schutz vor bedrohlichen Dateien über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie den Schutz vor bedrohlichen Dateien mithilfe der vordefinierten Aufgabe "Schutz vor bedrohlichen Dateien" (*File_Threat_Protection*) verwalten.

Die Aufgabe "Schutz vor bedrohlichen Dateien" wird standardmäßig gestartet. Sie können diese Aufgabe manuell starten und beenden.

Die Rechte der Administrator-Rolle sind erforderlich, um die Aufgabe zum Schutz vor bedrohlichen Dateien über die Befehlszeile zu starten und zu beenden.

Sie können die Einstellungen für den Schutz vor bedrohlichen Dateien konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zum Schutz vor bedrohlichen Dateien ändern.

Einstellungen der Aufgabe zum Schutz vor bedrohlichen Dateien

Die Tabelle beschreibt alle verfügbaren Werte und Standardwerte aller Einstellungen, die Sie für die Aufgabe zum Schutz vor bedrohlichen Dateien angeben können.

Einstellungen der Aufgabe zum Schutz vor bedrohlichen Dateien

Einstellung	Beschreibung	Werte
`ScanArchived`	Aktiviert die Untersuchung von Archiven (einschließlich selbstentpackender sfx-Archive). Die App untersucht Archive wie .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Die Liste der unterstützten Archivformate hängt von den verwendeten App-Datenbanken ab.	`Yes` – Archive untersuchen. Wenn der Wer `FirstAction=Recommended` angegeben ist, löscht die App je nach Archivtyp entweder das infizierte Objekt oder das gesamte Archiv, das die Bedrohung enthält `No` (Standardwert) – Archive nicht untersuchen.
`ScanSfxArchived`	Aktiviert die Untersuchung von	`Yes` – Selbstentpackende Archive

	nur selbstentpackenden Archiven (Archiven, zu deren Bestandteilen ein ausführbares Dekompressionsmodul gehört).	untersuchen. `No` (Standardwert) – Keine selbstentpackenden Archive untersuchen.
`ScanMailBases`	Aktiviert die Untersuchung von E-Mail-Datenbanken von Microsoft Outlook®, Outlook Express, The Bat und anderer Mail-Clients.	`Yes` – Dateien von E-Mail-Datenbanken untersuchen. `No` (Standardwert) – Dateien von E-Mail-Datenbanken nicht untersuchen.
`ScanPlainMail`	Aktiviert die Untersuchung von E-Mail-Nachrichten im Textformat (plain text).	`Yes` – E-Mail-Nachrichten im Textformat untersuchen. `No` (Standardwert) – E-Mail-Nachrichten ir Textformat nicht untersuchen.
`SkipPlainTextFiles`	Dateien im Textformat vorübergehend von der Untersuchung ausschließen. Wenn der Parameter den Wert `SkipPlainTextFiles=Yes` besitzt, untersucht die App keine Dateien im Textformat, wenn diese Dateien innerhalb von 10 Minuten nach der letzten Untersuchung von demselben Prozess erneut verwendet werden. Mit diesem Parameter können Sie die Untersuchung von Protokollen zur Ausführung der App optimieren.	`Yes` – Dateien im Textformat nicht untersuchen, wenn diese Dateien vom selben Prozess innerhalb von 10 Minuten nach der letzten Untersuchung wiederverwendet werden. `No` (Standardwert) – Dateien im Textforma werden untersucht.
`SizeLimit`	Maximale Größe des zu untersuchenden Objekts (in Megabyte). Wenn die Größe des zu untersuchenden Objekts den angegebenen Wert überschreitet, überspringt die App das Objekt während der Untersuchung.	0 – 999999 0 – Die App untersucht Objekte beliebiger Größe. Standardwert: 0.
`TimeLimit`	Maximale Untersuchungsdauer (in Sekunden) eines Objekts. Die App stellt die Untersuchung eines Objekts ein, wenn sie länger dauert als durch diese Einstellung festgelegt.	0 – 9999 0 – die Untersuchungsdauer für Objekte is nicht begrenzt. Standardwert: 60.
`FirstAction`	Auswahl der ersten Aktion, welche die App für infizierte Objekte ausführen soll.	`Disinfect` (desinfizieren) – Die App versucht, ein Objekt zu desinfizieren, und speichert eine Kopie davon im Backup-Speicher. Wenn die Desinfektion fehlschlä (beispielsweise, weil der Typ des Objekts oder der Typ der Bedrohung im Objekt nich desinfiziert werden kann), belässt die App das Objekt unverändert. Wenn die erste Aktion auf `Desinfizieren` festgelegt ist, wird empfohlen, die zweite Aktion mithilfe der Einstellung `SecondAction` anzugeben

		`Remove` (löschen) – Die App löscht das infizierte Objekt, nachdem eine Backup-Kopie davon erstellt wurde. `Recommended` (empfohlene Aktion ausführen) – Die App wählt automatisch eine Aktion für das Objekt und führt sie au wobei Informationen zu der im Objekt gefundenen Bedrohung berücksichtigt werden. Beispielsweise löscht Kaspersky Endpoint Security Trojaner sofort, da sie andere Dateien nicht infizieren und deshalb keine Desinfektion erfordern. `Block` (blockieren) – die App blockiert der Zugriff auf das infizierte Objekt. Informationen über das infizierte Objekt werden im Protokoll gespeichert. Standardwert: `Recommended`
`SecondAction`	Auswahl der zweiten Aktion, welche die App für infizierte Objekte ausführen soll. Die App führt die zweite Aktion aus, wenn die Ausführung der ersten Aktion misslingt.	Die Werte der Einstellung `SecondAction` sind dieselben wie die Werte der Einstellun `FirstAction`. Wenn als erste Aktion `Block` oder `Remove` ausgewählt ist, muss keine zweite Aktion angegeben werden. In allen anderen Fällen wird empfohlen, zwei Aktionen anzugeben. Wenn Sie keine zweite Aktion angegeben haben, wendet die App `Block` (blockieren) als zweite Aktion an. Standardwert: `Block`.
`UseExcludeMasks`	Aktiviert den Ausschluss von Objekten, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, von der Untersuchung.	`Yes` – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, aus der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht aus der Untersuchur ausschließen.

`ExcludeMasks.item_#`	Ausschluss von der Untersuchung von Objekten nach Name oder Maske.
	Mit dieser Einstellung können Sie eine einzelne Datei anhand des Namens oder mehrere Dateien anhand von Masken im Shell-Format aus dem angegebenen Untersuchungsbereich ausschließen.
		Der Standardwert ist nicht angegeben.
		Beispiel:
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Aktiviert den Ausschluss von Objekten mit Bedrohungen, die durch die Einstellung `ExcludeThreats.item_#` festgelegt sind, von der Untersuchung.	`Yes` – Objekte, die Bedrohungen enthalter die in der Einstellung `ExcludeThreats.item_#` angegeben sin von der Untersuchung ausschließen.

		`No` (Standardwert) – Objekte, die Bedrohungen enthalten, die in der Einstellung `ExcludeThreats.item_#` angegeben sind, nicht von der Untersuchur ausschließen.

`ExcludeThreats.item_#`	Schließt Objekte nach dem Namen der in den Objekten gefundenen Bedrohungen von der Untersuchung aus. Bevor Sie die Werte dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseExcludeThreats` aktiviert ist.
	
	Um ein Objekt von der Untersuchung auszuschließen, geben Sie den vollständigen Namen der Bedrohung an, die im Objekt gefunden wurde, d. h. die Zeile mit der Entscheidung der App, dass dieses Objekt infiziert ist.
	
	Sie können beispielsweise ein Tool zum Sammeln von Informationen über Ihr Netzwerk verwenden. Damit es von der App nicht blockiert wird, fügen Sie den vollständigen Namen der darin enthaltenen Bedrohung zur Liste der Bedrohungen hinzu, die von der Untersuchung ausgenommen sind.
	
	Den vollständigen Namen der im Objekt gefundenen Bedrohung finden Sie im Protokoll der App oder auf der Website https://threats.kaspersky.com.
		Beim Wert der Einstellung muss die Groß- und Kleinschreibung beachtet werden.
		
		Der Standardwert ist nicht angegeben.
		
		Beispiel:
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`ReportCleanObjects`	Aktiviert die Protokollierung von Informationen zu untersuchten Objekten, welche die App als nicht infiziert einstuft. Sie können diese Einstellung aktivieren, um beispielsweise sicherzustellen, dass ein bestimmtes Objekt durch die App untersucht wurde.	`Yes` – Informationen zu nicht infizierten Objekten im Protokoll speichern. `No` (Standardwert) – Informationen zu nich infizierten Objekten nicht im Protokoll speichern.
`ReportPackedObjects`	Aktiviert das Protokollieren von Informationen über untersuchte Objekte, die Bestandteil zusammengesetzter Objekte sind.	`Yes` – Informationen über die Untersuchur von Objekten, die zu einem Archiv gehören im Protokoll speichern. `No` (Standardwert) – Informationen über d Untersuchung von Objekten, die zu einem Archiv gehören, nicht im Protokoll speicher

	Sie können diese Einstellung aktivieren, um beispielsweise sicherzustellen, dass ein bestimmtes Objekt innerhalb eines Archivs von der App untersucht wurde.	
`ReportUnprocessedObjects`	Aktiviert das Protokollieren von Informationen über Objekte, die aus einem bestimmten Grund nicht verarbeitet wurden.	`Yes` – Informationen zu nicht verarbeiteten Objekten im Protokoll speichern. `No` (Standardwert) – Informationen zu nicht verarbeiteten Objekten nicht im Protokoll speichern.
`UseAnalyzer`	Aktiviert die heuristische Analyse. Mithilfe der heuristischen Analyse kann die App Bedrohungen bereits erkennen, bevor sie den Virenanalysten bekannt sind.	`Yes` (Standardwert) – Heuristische Analyse aktivieren. `No` – Heuristische Analyse deaktivieren.
`HeuristicLevel`	Legt die Stufe der heuristischen Analyse fest. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Gründlichkeit der Suche nach Bedrohungen, der Belastung der Betriebssystemressourcen und der Untersuchungsdauer. Je höher die festgelegte Ebene der heuristischen Analyse, desto mehr Ressourcen verbraucht die Untersuchung und desto länger dauert sie.	`Light` – Oberflächlichste Untersuchung mit minimaler Belastung des Systems. `Medium` – Mittlere Ebene der heuristischen Analyse mit ausgeglichener Belastung des Betriebssystems. `Deep` – Gründlichste Untersuchung mit maximaler Belastung des Betriebssystems. `Recommended` (Standardwert) – Der empfohlene Wert.
`UseIChecker`	Aktiviert die Nutzung der iChecker-Technologie.	`Yes` (Standardwert) – Nutzung der iChecker-Technologie aktivieren. `No` – Nutzung der iChecker-Technologie deaktivieren.
`ScanByAccessType`	Ausführungsmodus der Aufgabe zum Schutz vor bedrohlichen Dateien. Die Einstellung `ScanByAccessType` wird nur in der Aufgabe zum Schutz vor bedrohlichen Dateien verwendet.	`SmartCheck` (Standardwert) – die Datei wird beim Öffnen und erneut beim Schließen untersucht, falls sie geändert wurde. Wenn ein Prozess während seiner Ausführung in einem bestimmten Zeitraum mehrmals auf die Datei zugreift und diese verändert, wird diese Datei erst beim letzten Versuch des Prozesses, die Datei zu schließen, untersucht. `OpenAndModify` – die Datei wird beim Öffnen und erneut beim Schließen untersucht, falls sie geändert wurde. `Open` – die Datei wird beim Öffnen zum Lesen sowie beim Ausführen oder Ändern untersucht.

Der Abschnitt **[ScanScope.item_#]** enthält die folgenden Parameter:

	Beschreibung des	

`AreaDesc`	Untersuchungsbereichs mit zusätzlichen Informationen über den Untersuchungsbereich. Die maximale Länge einer Zeichenfolge, die mit dieser Einstellung angegeben werden kann, beträgt 4096 Zeichen.	Standardwert: `All objects`. Beispiel: `AreaDesc="Mail-Datenbanken untersuchen"`
`UseScanArea`	Aktiviert die Untersuchung des angegebenen Bereichs. Um die Aufgabe auszuführen, müssen Sie mindestens einen zu untersuchenden Bereich angeben.	`Yes` (Standardwert) – Den angegebenen Bereich untersuchen. `No` – Angegebenen Bereich nicht untersuchen.
`AreaMask.item_#`	Einschränkung des Untersuchungsbereichs. Im Untersuchungsbereich untersucht die APP nur Dateien, die mit Masken im Shell-Format angegeben wurden. Wenn die Einstellung nicht angegeben wurde, untersucht die App alle Objekte im Untersuchungsbereich. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: * (alle Objekte untersucher Beispiel: `AreaMask_item_<Nummer des Elements>=*doc`
`Path`	Pfad zum Verzeichnis mit untersuchten Objekten.	`<Pfad zum lokalen Verzeichnis>` – Objekte im angegebenen Verzeichnis untersuchen. Bei der Angabe des Pfades können Sie Masken und Tags verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>]`

`[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

`Shared:NFS` – Ressourcen des Gerätedateisystems untersuchen, auf die über das NFS-Protokoll zugegriffen wird.

`Shared:SMB` – Ressourcen des Gerätedateisystems untersuchen, auf die über das Samba-Protokoll zugegriffen wird

`Mounted:NFS` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über NFS-Protokoll eingebunden sind.

`Mounted:SMB` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über das Samba-Protokoll eingebunden sind.

`AllRemoteMounted` – alle Remote-Verzeichnisse untersuchen, die auf dem Gerät über Samba- oder NFS-Protokolle gemountet sind.

		`AllShared` – Ressourcen des Gerätedateisystems untersuchen, auf die über das Samba- und NFS-Protokoll zugegriffen wird. `< Typ des Dateisystems >` – alle Ressourcen des angegebenen Dateisysten des Geräts untersuchen.
Der Abschnitt **[ExcludedFromScanScope.item_#]** enthält die folgenden Parameter:		
`AreaDesc`	Beschreibung des Ausschlussbereichs von der Untersuchung mit zusätzlichen Informationen über den Ausschlussbereich.	Der Standardwert ist nicht angegeben.
`UseScanArea`	Schließt den angegebenen Bereich von der Untersuchung aus.	`Yes` (Standardwert) – Den angegebenen Bereich ausschließen. `No` – Den angegebenen Bereich nicht ausschließen.
`AreaMask.item_#`	Einschränkung des von der Untersuchung ausgeschlossenen Bereichs. Im Ausschlussbereich untersucht die App nur Dateien, die mit Masken im Shell-Format angegeben wurden. Wenn die Einstellung nicht angegeben wurde, schließt die App alle Objekte im Ausschlussbereich von der Untersuchung aus. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: `*` (alle Objekte von der Untersuchung ausschließen)
`Path`	Pfad zum Verzeichnis mit ausgeschlossenen Objekten.	`< Pfad zum lokalen Verzeichnis >` – Objekte im angegebenen Verzeichnis (und dessen Unterverzeichnissen) von der Untersuchung ausschließen. Bei der Angab des Pfades können Sie Masken und Tags verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>]`

		`[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. `Mounted:NFS` – Remote-Verzeichnisse, di auf dem Gerät über das NFS-Protokoll gemountet sind, von der Untersuchung ausschließen. `Mounted:SMB` – Remote-Verzeichnisse, di auf dem Gerät über das Samba-Protokoll gemountet sind, von der Untersuchung ausschließen. `AllRemoteMounted` – Alle Remote-Verzeichnisse, die auf dem Gerät über Samba- oder NFS-Protokolle gemountet sind, von der Untersuchung ausschließen. `<Typ des Dateisystems>` – alle Ressourcen des angegebenen Dateisysten des Geräts von der Untersuchung ausschließen.

Der Abschnitt **[ExcludedForProgram.item_#]** enthält die folgenden Einstellungen:

`ProgramPath`	Pfad des auszuschließenden Prozesses.	`<vollständiger Pfad des Prozesses>` – Prozess im angegebenen Verzeichnis von der Untersuchung ausschließen.
`ApplyToDescendants`	Untergeordnete Prozesse des ausgeschlossenen Prozesses, der durch den `ProgramPath`-Parameter angegeben ist, von der Untersuchung ausschließen.	`Yes` – Schließt den angegebenen Prozess und alle seine untergeordneten Prozesse von der Untersuchung aus. `No` (Standardwert) – Nur den angegebene Prozess von der Untersuchung ausschließe untergeordnete Prozesse nicht von der Untersuchung ausschließen.
`AreaDesc`	Beschreibung des Ausschlussbereichs von Prozessen.	Standardwert: `All objects`.
`UseExcludedForProgram`	Schließt den angegebenen Bereich von der Untersuchung aus.	`Yes` (Standardwert) – Den angegebenen Bereich ausschließen. `No` – Den angegebenen Bereich nicht ausschließen.
`AreaMask.item_#`	Einschränkung des Ausschlussbereichs von Prozessen. Im Ausschlussbereich für Prozesse werden von der App nur die Dateien nicht untersucht, die mithilfe von Masken im Shell-Format angegeben wurden. Wenn kein Parameter angegeben wurde, werden von der App alle Objekte im Ausschlussbereich von der Untersuchung ausgeschlossen. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: `*` (alle Objekte von der Untersuchung ausschließen)
`Path`	Pfad des Verzeichnisses mit Dateien, die der Prozess ändert.	`<Pfad zum lokalen Verzeichnis>` – Objekte im angegebenen Verzeichnis von der Untersuchung ausschließen. Bei der Angabe des Pfades können Masken verwendet werden.

Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

`Shared:NFS` – Ressourcen des Gerätedateisystems, auf die über das NFS Protokoll zugegriffen wird, von der Untersuchung ausschließen.

`Shared:SMB` – Ressourcen des Gerätedateisystems, auf die über das SAMBA-Protokoll zugegriffen wird, von der Untersuchung ausschließen.

`Mounted:NFS` – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll gemountet sind, von der Untersuchung ausschließen.

`Mounted:SMB` – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll gemountet sind, von der Untersuchung ausschließen.

`AllRemoteMounted` – Alle Remote-Verzeichnisse, die auf dem Gerät über Samba- oder NFS-Protokolle gemountet sind, von der Untersuchung ausschließen.

`AllShared` – Alle Ressourcen des Gerätedateisystems, auf die über Samba- oder NFS-Protokolle zugegriffen wird, von der Untersuchung ausschließen.

		< Typ des Dateisystems > – alle Ressourcen des angegebenen Dateisysten des Geräts von der Untersuchung ausschließen.

Optimierung der Überprüfung von Netzwerkverzeichnissen

Um die Ausführung des Schutzes vor bedrohlichen Dateien zu optimieren, können Sie den Ausschluss von Dateien, die aus Netzwerkverzeichnissen kopiert wurden, von der Untersuchung konfigurieren. Dazu müssen Sie einen Ausschluss nach Prozess für das Tool konfigurieren, das zum Kopieren aus Netzwerkverzeichnissen bestimmt ist (z. B. für das Tool `cp`).

So konfigurieren Sie den Ausschluss von Netzwerkverzeichnissen aus der Untersuchung:

1. Geben Sie die Einstellungen der Aufgabe "Schutz vor bedrohlichen Dateien" (*File Threat Protection*, ID:1) mit dem folgenden Befehl in der Konfigurationsdatei aus:

   ```
   kesl-control --get-settings 1 --file <vollständiger Pfad der Konfigurationsdatei> [--json]
   ```

2. Öffnen Sie die Konfigurationsdatei und fügen Sie den Abschnitt `[ExcludedForProgram.item_#]` mit den folgenden Einstellungen hinzu:

   - `ProgramPath` – Pfad des auszuschließenden Prozesses oder eines Verzeichnisses mit auszuschließenden Prozessen.
   - `ApplyToDescendants` – Einstellung, die angibt, ob untergeordnete Prozesse von der Untersuchung des auszuschließenden Prozesses auszuschließen sind (mögliche Werte: `Yes` oder `No`).
   - `AreaDesc` – Beschreibung des Ausschlussbereichs für Prozesse, die zusätzliche Informationen zum Ausschlussbereich enthält.
   - `UseExcludedForProgram` – Ausschluss des angegebenen Bereichs aktivieren, wenn die Aufgabe ausgeführt wird (mögliche Werte: `Ja` oder `Nein`).
   - `Path` – Pfad des Verzeichnisses mit Dateien, die der Prozess ändert.
   - `AreaMask.item_#` – Maske von Dateinamen für Dateien, die von der Untersuchung ausgeschlossen werden sollen. Sie können auch den vollständigen Pfad zur Datei angeben.

     Beispiel:

     ```
     [ExcludedForProgram.item_0000]
     ProgramPath=/usr/bin/cp
     ApplyToDescendants=No
     AreaDesc=
     UseExcludedForProgram=Yes
     Path=AllRemoteMounted
     AreaMask.item_0000=*
     ```

3. Führen Sie den Befehl aus:

   ```
   kesl-control --set-settings 1 --file <vollständiger Pfad der Konfigurationsdatei> [--json]
   ```

   Geben Sie den Schalter `--json` an, wenn Sie Einstellungen aus einer Konfigurationsdatei im JSON-Format importieren. Wenn Sie keinen Schalter angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Die App untersucht keine Dateien in Netzwerkverzeichnissen. Allerdings werden der Befehl `cp` (für das oben genannte Beispiel) und lokale Dateien untersucht.

Besonderheiten der Untersuchung von symbolischen Links und festen Links

Kaspersky Endpoint Security ermöglicht die Untersuchung symbolischer und fester Links zu Dateien.

Untersuchung von symbolischen Links

Die App untersucht symbolische Links nur dann, wenn die Datei, auf die der symbolische Link verweist, zum Untersuchungsbereich der Komponente zum Schutz vor bedrohlichen Dateien gehört.

Wenn die vom symbolischen Link referenzierte Datei nicht in dem Untersuchungsbereich der Komponente zum Schutz vor bedrohlichen Dateien fällt, führt die App keine Untersuchung dieser Datei durch. Sollte die Datei jedoch bösartigen Code enthalten, ist die Sicherheit des Geräts gefährdet.

Untersuchung von festen Links

Bei der Verarbeitung einer Datei mit mehr als einem festen Link wählt die App eine Aktion entsprechend der angegebenen Aktion für Objekte:

- Wenn die Aktion **Empfohlene Aktion ausführen** ausgewählt wurde, wählt die App die Aktion mit dem Objekt automatisch auf Basis von Informationen zum Risikowert der im Objekt gefundenen Bedrohung und zur Möglichkeit seiner Desinfektion aus und wendet diese an.

- Wenn die Aktion **Entfernen** ausgewählt wurde, löscht die App den zu verarbeitenden festen Link. Die übrigen festen Links zu dieser Datei werden nicht verarbeitet.

- Wenn Sie **Desinfizieren** auswählen, desinfiziert die App die Quelldatei. Wenn keine Desinfektion möglich ist, löscht die App den festen Link und erstellt stattdessen eine Kopie der Quelldatei mit dem Namen des entfernten festen Links.

Wenn Sie die Datei mit dem festen Link aus dem Backup wiederherstellen, erstellt die App eine Kopie der Quelldatei mit dem Namen des festen Links, die in das Backup verschoben wurde. Verknüpfungen mit den anderen harten Links zur Quelldatei werden nicht wiederhergestellt.

Schadsoftware-Untersuchung

Schadsoftware-Untersuchung – Eine auf Befehl ausgeführte, einmalige vollständige oder benutzerdefinierte Untersuchung der Dateien auf einem Gerät. Kaspersky Endpoint Security kann mehrere Aufgaben zur Schadsoftware-Untersuchung gleichzeitig ausführen.

Die App erstellt eine vordefinierte Aufgabe vom Typ *Schadsoftware-Untersuchung (Scan_My_Computer)*. Mit dieser Aufgabe können Sie eine vollständige Untersuchung des Geräts durchführen. Bei der vollständigen Untersuchung untersucht die App alle Objekte, die sich auf den lokalen Laufwerken des Geräts befinden, sowie alle gemounteten und freigegebenen Objekte, auf welche der Zugriff über die Protokolle Samba und NFS mit den empfohlenen Sicherheitseinstellungen erfolgt.

In Kaspersky Security Center erstellt der Assistent für die Ersteinrichtung von Kaspersky Security Center nach der Installation des MMC-Plug-ins oder des Web-Plug-ins für die Verwaltung von Kaspersky Endpoint Security automatisch eine Gruppenaufgabe zur Schadsoftware-Untersuchung.

Während der vollständigen Festplattenuntersuchung wird die CPU ausgelastet sein. Es wird empfohlen, die vollständige Festplattenuntersuchung durchzuführen, wenn sich das System im Ruhezustand befindet.

Sie können Einstellungen für automatisch erstellte Aufgaben in Kaspersky Security Center und über die Befehlszeile konfigurieren sowie Benutzeraufgaben zur Schadsoftware-Untersuchung erstellen.

Wenn Schadsoftware entdeckt wird, kann Kaspersky Endpoint Security die infizierte Datei löschen und den von dieser Datei gestarteten schädlichen Prozess beenden.

Wenn die App während Schadsoftware-Untersuchung von einem Kontrolldienst oder vom Benutzer manuell neu gestartet wurde, wird die Aufgabenausführung unterbrochen. Die App protokolliert dann das Ereignis *OnDemandTaskInterrupted*.

Sie können Aufgaben zur Schadsoftware-Untersuchung starten und Untersuchungseinstellungen konfigurieren:

- Wählen Sie Betriebssystemobjekte aus, die untersucht werden müssen: Dateien, Archive, Bootsektoren, Prozess- und Kernelspeicher sowie Autostart-Objekte.
- Begrenzen Sie die Größe des untersuchten Objekts und die Untersuchungsdauer für das Objekt.
- Wählen Sie die Aktionen aus, welche die App für infizierte Objekte ausführen soll.
- Konfigurieren Sie den Ausschluss von Objekten von der Untersuchung nach:
  - Namen oder Masken
  - Namen der in den Objekten gefundenen Bedrohungen
- Aktivieren oder deaktivieren der Verwendung von globalen Ausnahmen und von Ausnahmen aus dem Schutz vor bedrohlichen Dateien während der Untersuchung.
- Aktivieren Sie die Protokollierung von Informationen zu untersuchten nicht infizierten Objekten, zu untersuchten Objekten in Archiven und zu nicht verarbeiteten Objekten.
- Konfigurieren Sie die Verwendung der heuristischen Analyse und der iChecker-Technologie während der Untersuchung.
- Beschränken Sie die Anzahl der Geräte, deren Bootsektoren untersucht werden müssen.

- Konfigurieren Sie Untersuchungsbereiche und von der Untersuchung auszuschließende Bereiche.

Schadsoftware-Untersuchung in der Web Console

In der Web Console können Sie mithilfe der Aufgabe *Schadsoftware-Untersuchung* nach Schadsoftware suchen.

Sie können eine automatisch erstellte Gruppenaufgabe starten sowie Benutzeraufgaben für die Untersuchung erstellen und starten. Sie können die Untersuchungseinstellungen anpassen, indem Sie die Einstellungen der Aufgaben zur Schadsoftware-Untersuchung ändern.

Untersuchungsparameter der Aufgabe zur Schadsoftware-Untersuchung

Einstellung	Beschreibung
Archive untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Archiven. Wenn das Kontrollkästchen aktiviert ist, so untersucht die App Archive. Um ein Archiv zu untersuchen, muss es zunächst von der App entpackt werden, was die Untersuchung verlangsamen kann. Sie können die Dauer der Untersuchung von Archiven reduzieren, indem Sie im Abschnitt **Allgemeine Untersuchungseinstellungen** die Einstellungen **Dateien überspringen, deren Untersuchung länger dauert als (Sek.)** und/oder **Dateien überspringen, die größer sind als (MB)** konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Archive. Das Kontrollkästchen ist standardmäßig aktiviert.
Selbstentpackende Archive untersuchen	Das Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung *selbstentpackender Archive (self-extracting archives)*. Selbstentpackende Archive sind Archive, die ein ausführbares Modul zum Entpacken enthalten. Wenn das Kontrollkästchen aktiviert ist, untersucht die App selbstentpackende Archive. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine selbstentpackenden Dateien. Dieses Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Archive untersuchen** deaktiviert ist. Das Kontrollkästchen ist standardmäßig aktiviert.
Mail-Datenbanken untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Mail-Datenbanken der Anwendungen Microsoft Outlook, Outlook Express, The Bat! und anderen E-Mail-Clients. Wenn das Kontrollkästchen aktiviert ist, untersucht die App die Dateien von Mail-Datenbanken. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Dateien von Mail-Datenbanken. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Dateien in Mail-Formaten untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Dateien von E-Mail-Nachrichten im Textformat (plain text). Wenn das Kontrollkästchen aktiviert ist, untersucht die App E-Mail-Nachrichten im Textformat. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App E-Mail-Nachrichten im Textformat nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Dateien überspringen, deren Untersuchung länger dauert als (Sek.)	In diesem Feld können Sie die erlaubte Höchstdauer für die Untersuchung der Datei in Sekunden angeben. Nach Ablauf des angegebenen Zeitraums bricht die App die Untersuchung der Datei ab. Zulässige Werte: 0–9999. Ist der Wert 0 angegeben, dann ist die Untersuchungsdauer nicht beschränkt. Standardwert: 0.
Dateien überspringen, die größer sind als (MB)	In diesem Feld können Sie die maximale Größe der untersuchten Datei in Megabyte angeben. Zulässige Werte: 0–999999. Ist der Wert 0 angegeben, untersucht die App Dateien jeder Größe. Standardwert: 0.
Virenfreie Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectProcessed*. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Unverarbeitete Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectNotProcessed*, wenn eine Datei während der Untersuchung nicht verarbeitet werden kann. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *ObjectNotProcessed*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *ObjectNotProcessed*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Gepackte Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *PackedObjectDetected* für alle erkannten gepackten Objekte. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *PackedObjectDetected*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *PackedObjectDetected*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
iChecker-Technologie verwenden	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung nur neuer oder seit der letzten Untersuchung geänderter Dateien. Wenn das Kontrollkästchen aktiviert ist, untersucht die App nur neue oder seit der letzten Untersuchung geänderte Dateien. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App Dateien unabhängig von ihrem Erstellungs- oder Änderungsdatum. Das Kontrollkästchen ist standardmäßig aktiviert.
Heuristische Analyse verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die heuristische Analyse bei der Untersuchung von Dateien. Das Kontrollkästchen ist standardmäßig aktiviert.
Stufe der heuristischen Analyse	Wenn das Kontrollkästchen **Heuristische Analyse verwenden** aktiviert ist, können Sie die Ebene der heuristischen Analyse in der Dropdown-Liste festlegen:

	• **Oberflächlich** – Die am wenigsten detaillierte Untersuchung, minimale Systembelastung. • **Mittel** – Mittlere Untersuchung, ausgeglichene Systembelastung. • **Tief** – Detaillierteste Untersuchung, maximale Systembelastung. • **Empfohlen** (Standardwert) – Optimale Stufe, die von den Kaspersky-Experten empfohlen wird. Sie bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Geräte.
Erste Aktion	In der Dropdown-Liste können Sie die erste Aktion auswählen, die von der App für das gefundene infizierte Objekt ausgeführt werden soll: • Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Informationen zur Gefahrenstufe der in der Datei erkannten Bedrohung und zur Möglichkeit ihrer Desinfektion (Standardwert). • Objekt **überspringen**.
Zweite Aktion	In dieser Dropdown-Liste können Sie die zweite Aktion auswählen, die von der App für ein infiziertes Objekt ausgeführt werden soll, falls die erste Aktion nicht erfolgreich war: • Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Daten zur in der Datei erkannten Gefahrenstufe der Bedrohung und zur Möglichkeit ihrer Desinfektion. • Objekt **überspringen** (Standardwert).
Untersuchungsbereiche	Eine Tabelle mit Bereichen, die von der Aufgabe untersucht werden sollen. Standardmäßig enthält die Tabelle einen Untersuchungsbereich, der alle Verzeichnisse des lokalen Dateisystems umfasst. Sie können Untersuchungsbereiche in der Tabelle hinzufügen, konfigurieren, löschen, nach oben verschieben und nach unten verschieben.

Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Ein Klick auf den Namen des Untersuchungsbereichs öffnet das Fenster **<Name des Untersuchungsbereichs>**. In diesem Fenster können Sie die Einstellungen des ausgewählten Untersuchungsbereichs ändern.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **<Neuer Untersuchungsbereich>**. In diesem Fenster können Sie einen neuen Untersuchungsbereich festlegen.

Fenster zum Hinzufügen des Untersuchungsbereichs

In diesem Fenster können Sie einen neuen Untersuchungsbereich hinzufügen oder anpassen.

Einstellungen des Untersuchungsbereichs

Einstellung	Beschreibung

Name des Bereichs	Eingabefeld für den Namen der Untersuchungsbereichs. Dieser Name wird in der Tabelle **Untersuchungsbereiche** im Abschnitt **Untersuchungseinstellungen** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung dieses Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, verarbeitet die App diesen Untersuchungsbereich während ihrer Ausführung. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die App diesen Untersuchungsbereich während ihrer Ausführung nicht. Sie können diesen Bereich zu einem späteren Zeitpunkt zu den Betriebseinstellungen der Komponente hinzufügen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	In der Dropdown-Liste können Sie den Typ des Dateisystems auswählen: • **Lokal** (Standardwert) – Lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie den Pfad zu einem lokalen Verzeichnis angeben. • **Mounted** – Gemountete Remote-Verzeichnisse oder lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie das Protokoll oder den Namen des Dateisystems angeben. • **Freigegeben** – Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind. • **Alle freigegebenen** – Alle Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind.
Zugriffsprotokoll	In der Dropdown-Liste können Sie das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind. Diese Dropdown-Liste ist verfügbar, wenn in der Dropdown-Liste für Dateisysteme als Typ **Freigegeben** oder **Mounted** ausgewählt ist.
Pfad	Eingabefeld für den Pfad des Verzeichnisses, das in den Untersuchungsbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken und Tags verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

	Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardmäßige Pfadangabe **/** – Die App untersucht alle Verzeichnisse des lokalen Dateisystems. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Lokal** ausgewählt ist. Wenn in der Dropdown-Liste der Dateisysteme als Typ **Lokal** ausgewählt ist und kein Pfad angegeben wird, untersucht die App alle Verzeichnisse des lokalen Dateisystems.
Name der freigegebenen Ressource	Eingabefeld für den Namen der freigegebenen Ressource des Dateisystems, auf der sich die Verzeichnisse befinden, die Sie zum Untersuchungsbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste **Zugriffsprotokoll** das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der App während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster. Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Abschnitt "Untersuchungsbereiche"

Sie können die Einstellungen für den Untersuchungsbereich der Aufgabe zur Schadsoftware-Untersuchung anpassen. Die App ermöglicht die Untersuchung von Dateien, Bootsektoren, und Speicher des Client-Geräts, sowie von Autostart-Objekten.

Parameter für den Untersuchungsbereich der Aufgabe zur Schadsoftware-Untersuchung

Einstellung	Beschreibung
Dateien untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Dateien. Wenn das Kontrollkästchen aktiviert ist, untersucht die App Dateien. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Dateien. Das Kontrollkästchen ist standardmäßig aktiviert.
Bootsektoren untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Bootsektoren. Wenn das Kontrollkästchen aktiviert ist, untersucht die App Bootsektoren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Bootsektoren. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Kernelspeicher und gestartete Prozesse untersuchen.	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung des Arbeitsspeichers des Client-Geräts. Wenn diese Option aktiviert ist, überprüft die App den Kernel-Speicher und die gestarteten Prozesse. Wenn das Kontrollkästchen deaktiviert ist, überprüft die App den Kernel-Speicher und die gestarteten Prozesse nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Autostart-Objekte untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Autostart-Objekten. Wenn das Kontrollkästchen aktiviert ist, untersucht die App Autostart-Objekte. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Autostart-Objekte. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Zu untersuchende Geräte	Der Link **Gerätemasken** anpassen öffnet das Fenster **Untersuchungsbereiche**. In diesem Fenster können Sie die Geräte angeben, deren Bootsektoren untersucht werden sollen.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält die Masken der Gerätenamen, deren Bootsektoren die App untersuchen soll. Standardmäßig enthält die Tabelle die Gerätenamen-Maske **/**** (alle Geräte).

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Abschnitt "Ausschlussbereiche"

Im Abschnitt **Ausschlussbereiche** der Aufgabe "Schadsoftware-Untersuchung" können Sie die Ausschlussbereiche, die Ausschlüsse nach Maske und Bedrohungsname sowie die Verwendung globaler Ausschlüsse und Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der Ausführung der Aufgabe konfigurieren.

Einstellungen der Ausschlüsse von der Untersuchung

Einstellung	Beschreibung
Ausschlussbereich anpassen	Der Link **Ausschlussbereiche anpassen** öffnet das Fenster **Ausschlussbereiche**. In diesem Fenster können Sie eine Liste mit Ausschlüsse von der Untersuchung festlegen.
Ausschlüsse nach Maske anpassen	Der Link **Ausschlüsse nach Maske anpassen** öffnet das Fenster **Ausschlüsse nach Maske**. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren.
Ausschlüsse nach Bedrohungsname anpassen	Der Link **Ausschlüsse nach Bedrohungsname anpassen** öffnet das Fenster **Ausschlüsse nach Bedrohungsname**. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren.
Globale Ausnahmen verwenden	Das Kontrollkästchen aktiviert oder deaktiviert den Ausschluss von in den globalen Ausnahmen angegeben Mountpunkten während der App-Ausführung. Wenn diese Option aktiviert ist, schließt die App die konfigurierten Mountpunkte von der Untersuchung aus. Das Kontrollkästchen ist standardmäßig aktiviert.
Ausschlüsse aus dem Schutz vor bedrohlichen Dateien verwenden	Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung konfigurierter Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der App-Ausführung. Wenn das Kontrollkästchen aktiviert ist, schließt die App jene Objekte von der Untersuchung aus, die in den Ausschlüssen der Komponente "Schutz vor bedrohlichen Dateien" angegeben sind. Das Kontrollkästchen ist standardmäßig aktiviert.

Fenster "Ausschlussbereiche"

Die Tabelle enthält Bereiche mit Ausschlüsse von der Untersuchung. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der App angewendet wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster zum Hinzufügen des Ausschlussbereichs

In diesem Fenster können Sie einen neuen Ausschlussbereich hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster **Ausschlussbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss des Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, wird dieser Bereich während der Ausführung der App von der Untersuchung oder vom Schutz ausgeschlossen. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich während der Ausführung der App in die Untersuchung oder den Schutz eingeschlossen. Im Folgenden können Sie diesen Bereich von der Untersuchung oder dem Schutz ausschließen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	In der Dropdown-Liste können Sie den Typ des Dateisystems auswählen, auf dem sich die Verzeichnisse befinden, die Sie zu den Ausschlüssen von der Untersuchung hinzufügen möchten: • **Lokal** – Lokale Verzeichnisse.

	• **Mounted** – Remote-Verzeichnisse, die auf dem Gerät eingebunden sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind.
Zugriffsprotokoll	In der Dropdown-Liste können Sie das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind. Diese Dropdown-Liste ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** ausgewählt ist.
Pfad	Eingabefeld für den Pfad des Verzeichnisses, das in den Ausschlussbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken und Tags verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

	Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Als Pfad ist standardmäßig **/** angegeben: Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Lokal** ausgewählt ist.
Name der freigegebenen Ressource	Eingabefeld für den Namen der freigegebenen Ressource des Dateisystems, auf der sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten: Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste **Zugriffsprotokoll** das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Untersuchung ausgeschlossen werden. Die Masken werden nur innerhalb des Verzeichnisses übernommen, das im Eingabefeld **Pfad** angegeben ist. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen. Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist. Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Maske"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren. Die App untersucht keine Dateien, deren Namen die angegebenen Masken enthalten. Standardmäßig ist die Liste mit Masken leer.

Sie können Masken hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist.

Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Bedrohungsname"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren. Die App blockiert die angegebenen Bedrohungen nicht. Standardmäßig ist die Liste mit den Namen von Bedrohungen leer.

Sie können Namen von Bedrohungen hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Bedrohung aus den Ausschlüsse.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens ein Bedrohungsname ausgewählt ist.

Ein Klick auf den Namen einer Bedrohung in der Tabelle öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung ändern, die von der Untersuchung ausgenommen wird.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung angeben, die von der Untersuchung ausgenommen wird.

Schadsoftware-Untersuchung in der Verwaltungskonsole

In der Verwaltungskonsole können Sie mithilfe der Aufgabe *Schadsoftware-Untersuchung* nach Schadsoftware suchen.

Sie können eine automatisch erstellte Gruppenaufgabe starten sowie Benutzeraufgaben für die Untersuchung erstellen und starten. Sie können die Untersuchungseinstellungen anpassen, indem Sie die Einstellungen der Aufgaben zur Schadsoftware-Untersuchung ändern.

Im Abschnitt **Einstellungen** in den Eigenschaften der Aufgabe "Schadsoftware-Untersuchung" können Sie die in der folgenden Tabelle aufgeführten Einstellungen konfigurieren.

Parameter der Aufgabe zur Schadsoftware-Untersuchung

Einstellung	Beschreibung
Untersuchung	Diese Einstellungsgruppe enthält Schaltflächen, mit denen Fenster geöffnet werden können, in denen Sie die Untersuchungsbereiche, die Einstellungen des Untersuchungsbereichs und die Untersuchungseinstellungen anpassen können.
Aktion beim Erkennen einer Bedrohung	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, mit der das Fenster **Aktionen beim Erkennen von Bedrohungen** geöffnet werden kann. In diesem Fenster können Sie die Aktionen konfigurieren, die von der App für das erkannte infizierte Objekt ausgeführt werden soll.

Im Abschnitt **Ausnahmen** in den Einstellungen der Aufgabe zur Schadsoftware-Untersuchung können Sie Ausschlussbereiche, Ausschlüsse nach Maske und Ausschlüsse nach Bedrohungsname anpassen.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält den Untersuchungsbereich. Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle einen Untersuchungsbereich, der alle Verzeichnisse des lokalen Dateisystems umfasst.

Einstellungen des Untersuchungsbereichs

Einstellung	Beschreibung

Name des Bereichs	Name des Untersuchungsbereichs
Pfad	Der Pfad zu dem zu untersuchenden Verzeichnis.
Status	Der Status gibt an, ob die App diesen Bereich während ihrer Ausführung untersucht.

Sie können Elemente in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.

Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Liste der Bereiche angeben sind. Um bei Bedarf für das Unterverzeichnis andere Sicherheitseinstellungen festzulegen als für das übergeordnete Verzeichnis, platzieren Sie erforderlichenfalls das Unterverzeichnis in der Liste über dem übergeordneten Verzeichnis.

Fenster "<Neuer Untersuchungsbereich>"

In diesem Fenster können Sie einen neuen Untersuchungsbereich hinzufügen oder anpassen.

Einstellungen des Untersuchungsbereichs

Einstellung	Beschreibung
Name des	Eingabefeld für den Namen der Untersuchungsbereichs. Dieser Name wird in der

Untersuchungsbereichs	Tabelle im Fenster **Untersuchungsbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung dieses Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, verarbeitet die App diesen Untersuchungsbereich während ihrer Ausführung. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die App diesen Untersuchungsbereich während ihrer Ausführung nicht. Sie können diesen Bereich zu einem späteren Zeitpunkt zu den Betriebseinstellungen der Komponente hinzufügen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Diese Einstellungsgruppe ermöglicht die Konfiguration des Untersuchungsbereichs. In der Dropdown-Liste der Dateisysteme können Sie den Typ des Dateisystems auswählen: • **Lokal** (Standardwert) – Lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie den Pfad zu einem lokalen Verzeichnis angeben. • **Mounted** – Gemountete Remote-Verzeichnisse oder lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie das Protokoll oder den Namen des Dateisystems angeben. • **Freigegeben** – Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind. • **Alle freigegebenen** – Alle Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind.
	Wenn in der Drop-down-Liste der Dateisysteme der Typ **Alle** oder **Mounted** ausgewählt ist, können Sie rechts in der Drop-down-Liste das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind.
	Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Untersuchungsbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie Masken und Tags verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

	Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardmäßige Pfadangabe **/** – Die App untersucht alle Verzeichnisse des lokalen Dateisystems. Wenn in der Dropdown-Liste der Dateisysteme als Typ **Lokal** ausgewählt ist und kein Pfad angegeben wird, untersucht die App alle Verzeichnisse des lokalen Dateisystems.
Name des Dateisystems	Eingabefeld für den Namen des Dateisystems, auf dem sich die Verzeichnisse befinden, die Sie zum Untersuchungsbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste auf der rechten Seite das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der App während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster. Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Einstellungen des Untersuchungsbereichs"

In diesem Fenster können Sie die Einstellungen für die Untersuchung während der Ausführung der Aufgabe zur Schadsoftware-Untersuchung konfigurieren. Die App ermöglicht die Untersuchung von Dateien, Bootsektoren, Gerätespeicher und Autostart-Objekten.

Einstellungen des Untersuchungsbereichs

Einstellung	Beschreibung
Dateien untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Dateien. Wenn das Kontrollkästchen aktiviert ist, untersucht die App Dateien. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Dateien. Das Kontrollkästchen ist standardmäßig aktiviert.
Bootsektoren untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Bootsektoren. Wenn das Kontrollkästchen aktiviert ist, untersucht die App Bootsektoren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Bootsektoren. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Kernelspeicher und gestartete Prozesse untersuchen.	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung des Arbeitsspeichers des Geräts. Wenn diese Option aktiviert ist, überprüft die App den Kernel-Speicher und die gestarteten Prozesse. Wenn das Kontrollkästchen deaktiviert ist, überprüft die App den Kernel-Speicher und die gestarteten Prozesse nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Autostart-Objekte untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Autostart-Objekten. Wenn das Kontrollkästchen aktiviert ist, untersucht die App Autostart-Objekte. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Autostart-Objekte. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Zu untersuchende Geräte	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Untersuchungsbereiche** öffnet. In diesem Fenster können Sie die Geräte angeben, deren Bootsektoren untersucht werden sollen.
Globale Ausnahmen verwenden	Das Kontrollkästchen aktiviert oder deaktiviert den Ausschluss von in den globalen Ausnahmen angegeben Mountpunkten während der App-Ausführung. Wenn diese Option aktiviert ist, schließt die App die konfigurierten Mountpunkte von der Untersuchung aus. Das Kontrollkästchen ist standardmäßig aktiviert.
Ausschlüsse aus dem Schutz vor bedrohlichen Dateien verwenden	Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung konfigurierter Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der App-Ausführung. Wenn das Kontrollkästchen aktiviert ist, schließt die App jene Objekte von der Untersuchung aus, die in den Ausschlüssen der Komponente "Schutz vor bedrohlichen Dateien" angegeben sind.

	Das Kontrollkästchen ist standardmäßig aktiviert.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält die Masken der Gerätenamen, deren Bootsektoren die App untersuchen soll. Standardmäßig enthält die Tabelle die Gerätenamen-Maske **/**** (alle Geräte).

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Untersuchungseinstellungen"

In diesem Fenster können Sie die Einstellungen für die Untersuchung von Dateien durch die Aufgabe konfigurieren.

Untersuchungseinstellungen

Einstellung	Beschreibung
Archive untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Archiven. Wenn das Kontrollkästchen aktiviert ist, so untersucht die App Archive. Um ein Archiv zu untersuchen, muss es zunächst von der App entpackt werden, was die Untersuchung verlangsamen kann. Sie können die Dauer der Untersuchung von Archiven reduzieren, indem Sie im Abschnitt **Allgemeine Untersuchungseinstellungen** die Einstellungen **Dateien überspringen, deren Untersuchung länger dauert als (Sek.)** und/oder **Dateien überspringen, die größer sind als (MB)** konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Archive. Das Kontrollkästchen ist standardmäßig aktiviert.
Selbstentpackende Archive untersuchen	Das Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung *selbstentpackender Archive (self-extracting archives)*. Selbstentpackende Archive sind Archive, die ein ausführbares Modul zum Entpacken enthalten. Wenn das Kontrollkästchen aktiviert ist, untersucht die App selbstentpackende Archive. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine selbstentpackenden Dateien. Dieses Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Archive untersuchen** deaktiviert ist.

	Das Kontrollkästchen ist standardmäßig aktiviert.
Mail-Datenbanken untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Mail-Datenbanken der Anwendungen Microsoft Outlook, Outlook Express, The Bat! und anderen E-Mail-Clients. Wenn das Kontrollkästchen aktiviert ist, untersucht die App die Dateien von Mail-Datenbanken. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Dateien von Mail-Datenbanken. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Dateien in Mail-Formaten untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Dateien von E-Mail-Nachrichten im Textformat (plain text). Wenn das Kontrollkästchen aktiviert ist, untersucht die App E-Mail-Nachrichten im Textformat. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App E-Mail-Nachrichten im Textformat nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Dateien überspringen, deren Untersuchung länger dauert als (Sek.)	In diesem Feld können Sie die erlaubte Höchstdauer für die Untersuchung der Datei in Sekunden angeben. Nach Ablauf des angegebenen Zeitraums bricht die App die Untersuchung der Datei ab. Zulässige Werte: 0–9999. Ist der Wert 0 angegeben, dann ist die Untersuchungsdauer nicht beschränkt. Standardwert: 0.
Dateien überspringen, die größer sind als (MB)	In diesem Feld können Sie die maximale Größe der untersuchten Datei in Megabyte angeben. Zulässige Werte: 0–999999. Ist der Wert 0 angegeben, untersucht die App Dateien jeder Größe. Standardwert: 0.
Virenfreie Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectProcessed*. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Unverarbeitete Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectNotProcessed*, wenn eine Datei während der Untersuchung nicht verarbeitet werden kann. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *ObjectNotProcessed*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *ObjectNotProcessed*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Gepackte Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *PackedObjectDetected* für alle erkannten gepackten Objekte. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *PackedObjectDetected*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *PackedObjectDetected*.

	Dieses Kontrollkästchen ist standardmäßig deaktiviert.
iChecker-Technologie verwenden	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung nur neuer oder seit der letzten Untersuchung geänderter Dateien. Wenn das Kontrollkästchen aktiviert ist, untersucht die App nur neue oder seit der letzten Untersuchung geänderte Dateien. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App Dateien unabhängig von ihrem Erstellungs- oder Änderungsdatum. Das Kontrollkästchen ist standardmäßig aktiviert.
Heuristische Analyse verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die heuristische Analyse bei der Untersuchung von Dateien. Das Kontrollkästchen ist standardmäßig aktiviert.
Stufe der heuristischen Analyse	Wenn das Kontrollkästchen **Heuristische Analyse verwenden** aktiviert ist, können Sie die Ebene der heuristischen Analyse in der Dropdown-Liste festlegen: • **Oberflächlich** – Die am wenigsten detaillierte Untersuchung, minimale Systembelastung. • **Mittel** – Mittlere Untersuchung, ausgeglichene Systembelastung. • **Tief** – Detaillierteste Untersuchung, maximale Systembelastung. • **Empfohlen** (Standardwert) – Optimale Stufe, die von den Kaspersky-Experten empfohlen wird. Sie bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Geräte.

Fenster "Aktion beim Fund einer Bedrohung"

In diesem Fenster können Sie Aktionen auswählen, die von der App Kaspersky Endpoint Security für gefundene infizierte Objekte ausgeführt werden soll.

Aktionen beim Fund einer Bedrohung

Einstellung	Beschreibung
Erste Aktion	In der Dropdown-Liste können Sie die erste Aktion auswählen, die von der App für das gefundene infizierte Objekt ausgeführt werden soll: • Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Informationen zur Gefahrenstufe der in der Datei erkannten Bedrohung und zur Möglichkeit ihrer Desinfektion (Standardwert). • Objekt **überspringen**.
Zweite Aktion	In dieser Dropdown-Liste können Sie die zweite Aktion auswählen, die von der App für ein infiziertes Objekt ausgeführt werden soll, falls die erste Aktion nicht erfolgreich war: • Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt.

	• Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Daten zur in der Datei erkannten Gefahrenstufe der Bedrohung und zur Möglichkeit ihrer Desinfektion. • Objekt **überspringen** (Standardwert).

Abschnitt "Ausnahmen"

Ausschluss von der Untersuchung – Eine Reihe von Bedingungen, die erfüllt sein müssen, damit die App Kaspersky Endpoint Security Objekte nicht auf Viren und andere Schadsoftware überprüft. Objekte können auch anhand von Masken und Bedrohungsnamen von der Untersuchung ausgeschlossen werden.

Einstellungen der Ausschlüsse von der Untersuchung

Einstellungsgruppe	Beschreibung
Ausschlussbereiche	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausschlussbereiche** öffnet. In diesem Fenster können Sie eine Liste mit Bereichen festlegen, die von der Untersuchung ausgeschlossen werden sollen.
Ausschlüsse nach Maske	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausschlüsse nach Maske** öffnet. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren.
Ausschlüsse nach Bedrohungsname	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausschlüsse nach Bedrohungsname** öffnet. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren.

Fenster "Ausschlussbereiche"

Die Tabelle enthält Bereiche mit Ausschlüsse von der Untersuchung. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der App angewendet wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "<Neuer Ausschlussbereich>"

In diesem Fenster können Sie einen neuen Bereich mit Untersuchungsausschlüssen hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster **Ausschlussbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss des Bereichs von der Untersuchung während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während ihrer Ausführung von der Untersuchung aus. Wenn das Kontrollkästchen deaktiviert ist, schließt die App diesen Bereich während ihrer Ausführung in die Untersuchung ein. Sie können diesen Bereich zu einem späteren Zeitpunkt ausschließen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Diese Einstellungsgruppe erlaubt die Konfiguration des Ausschlussbereichs. In der Dropdown-Liste der Dateisysteme können Sie den Typ des Dateisystems auswählen, auf dem sich die Verzeichnisse befinden, die von der Untersuchung ausgeschlossen werden sollen: • **Lokal** – Lokale Verzeichnisse. • **Mounted** – Eingebundene Verzeichnisse. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind.
	Wenn in der Drop-down-Liste der Dateisysteme der Typ **Mounted** ausgewählt ist, können Sie rechts in der Drop-down-Liste das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind.
	Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können

Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Ausschlussbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie Masken und Tags verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

	Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Als Pfad ist standardmäßig **/** angegeben: Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus.
Name des Dateisystems	Eingabefeld für den Namen des Dateisystems, auf dem sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste auf der rechten Seite das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Untersuchung ausgeschlossen werden. Die Masken werden nur auf Objekte innerhalb des Verzeichnisses angewendet, das im Eingabefeld des Pfades angegeben ist. Standardmäßig enthält die Liste die Maske ***** (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen. Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist. Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Maske"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren. Die App untersucht keine Dateien, deren Namen die angegebenen Masken enthalten. Standardmäßig ist die Liste mit Masken leer.

Sie können Masken hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist.

Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Bedrohungsname"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren. Die App blockiert die angegebenen Bedrohungen nicht. Standardmäßig ist die Liste mit den Namen von Bedrohungen leer.

Sie können Namen von Bedrohungen hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Bedrohung aus den Ausschlüsse.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens ein Bedrohungsname ausgewählt ist.

Ein Klick auf den Namen einer Bedrohung in der Tabelle öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung ändern, die von der Untersuchung ausgenommen wird.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung angeben, die von der Untersuchung ausgenommen wird.

Schadsoftware-Untersuchung über die Befehlszeile

Über die Befehlszeile können Sie auf folgende Arten eine Schadsoftware-Untersuchung durchführen:

- Mithilfe der vordefinierten Aufgabe "Schadsoftware-Untersuchung" (*Scan_My_Computer*). Sie können diese Aufgabe manuell starten, beenden, anhalten und fortsetzen und den Zeitplan für den Aufgabenstart konfigurieren. Sie können die Einstellungen für die Untersuchung konfigurieren, indem Sie die Einstellungen für diese Aufgabe ändern.

- Mithilfe von Benutzeraufgaben zur Schadsoftware-Untersuchung (Aufgaben vom Typ *ODS*). Sie können Benutzeraufgaben manuell starten, beenden, anhalten und fortsetzen und den Zeitplan für den Aufgabenstart konfigurieren.

- Mit dem Befehl `kesl-control --scan-file` können Sie eine *benutzerdefinierte Untersuchung* bestimmter Dateien und Verzeichnisse durchführen.

Einstellungen der vordefinierten Aufgabe zur Schadsoftware-Untersuchung

Die Tabelle beschreibt alle verfügbaren Werte und Standardwerte aller Parameter, die Sie für die Aufgabe zur Schadsoftware-Untersuchung angeben können.

Parameter der Aufgabe zur Schadsoftware-Untersuchung

Einstellung	Beschreibung	Werte
`ScanFiles`	Aktiviert die Untersuchung von Dateien.	`Yes` (Standardwert) – Dateien untersuche `No` – Dateien nicht untersuchen.
`ScanBootSectors`	Aktiviert die Untersuchung der Bootsektoren.	`Yes` (Standardwert) – Bootsektoren untersuchen. `No` – Bootsektoren nicht untersuchen.
`ScanComputerMemory`	Aktiviert die Untersuchung des Prozess- und Kernelspeichers.	`Yes` (Standardwert) – Prozess-Speicher und Kernelspeicher untersuchen.

		`No` – Prozess-Speicher und Kernelspeiche nicht untersuchen.
`ScanStartupObjects`	Aktiviert die Untersuchung der Autostart-Objekte.	`Yes` (Standardwert) – Autostart-Objekte untersuchen. `No` – Autostart-Objekte nicht untersucher
`ScanArchived`	Aktiviert die Untersuchung von Archiven (einschließlich selbstentpackender sfx-Archive). Die App untersucht Archive wie .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Die Liste der unterstützten Archivformate hängt von den verwendeten App-Datenbanken ab.	`Yes` (Standardwert) – Archive untersuche Wenn der Wert `FirstAction=Recommended` angegeben ist, löscht die App je nach Archivtyp entweder das infizierte Objekt oder das gesamte Archiv, das die Bedrohung enthält `No` – Archive nicht untersuchen.
`ScanSfxArchived`	Aktiviert die Untersuchung von nur selbstentpackenden Archiven (Archiven, zu deren Bestandteilen ein ausführbares Dekompressionsmodul gehört).	`Yes` (Standardwert) – Selbstentpackende Archive untersuchen. `No` – Selbstentpackende Archive nicht untersuchen.
`ScanMailBases`	Aktiviert die Untersuchung von E-Mail-Datenbanken von Microsoft Outlook, Outlook Express, The Bat und anderer Mail-Clients.	`Yes` – Dateien von E-Mail-Datenbanken untersuchen. `No` (Standardwert) – Dateien von E-Mail-Datenbanken nicht untersuchen.
`ScanPlainMail`	Aktiviert die Untersuchung von E-Mail-Nachrichten im Textformat (plain text).	`Yes` – E-Mail-Nachrichten im Textformat untersuchen. `No` (Standardwert) – E-Mail-Nachrichten ir Textformat nicht untersuchen.
`SizeLimit`	Maximale Größe des zu untersuchenden Objekts (in Megabyte). Wenn die Größe des zu untersuchenden Objekts den angegebenen Wert überschreitet, überspringt die App das Objekt während der Untersuchung.	0 – 999999 0 – Die App untersucht Objekte beliebiger Größe. Standardwert: 0.
`TimeLimit`	Maximale Untersuchungsdauer (in Sekunden) eines Objekts. Die App stellt die Untersuchung eines Objekts ein, wenn sie länger dauert als durch diese Einstellung festgelegt.	0 – 9999 0 – die Untersuchungsdauer für Objekte is nicht begrenzt. Standardwert: 0.
`FirstAction`	Auswahl der ersten Aktion, welche die App für infizierte Objekte ausführen soll.	`Disinfect` (desinfizieren) – Die App versucht, ein Objekt zu desinfizieren, und speichert eine Kopie davon im Backup-Speicher. Wenn die Desinfektion fehlschläg (beispielsweise, weil der Typ des Objekts oder der Typ der Bedrohung im Objekt nich desinfiziert werden kann), belässt die App das Objekt unverändert. Wenn die erste Aktion auf `Desinfizieren` festgelegt ist,

		wird empfohlen, die zweite Aktion mithilfe der Einstellung `SecondAction` anzugeben `Remove` (löschen) – Die App löscht das infizierte Objekt, nachdem eine Backup-Kopie davon erstellt wurde. `Recommended` (empfohlene Aktion ausführen) – Die App wählt automatisch eine Aktion für das Objekt und führt sie au wobei Informationen zu der im Objekt gefundenen Bedrohung berücksichtigt werden. Beispielsweise löscht Kaspersky Endpoint Security Trojaner sofort, da sie andere Dateien nicht infizieren und deshalb keine Desinfektion erfordern. `Skip` (überspringen) – Die App unternimm keinen Versuch, das infizierte Objekt zu desinfizieren oder zu löschen. Informatione über das infizierte Objekt werden im Protokoll gespeichert. Standardwert: `Recommended`
`SecondAction`	Auswahl der zweiten Aktion, welche die App für infizierte Objekte ausführen soll. Die App führt die zweite Aktion aus, wenn die Ausführung der ersten Aktion misslingt.	Die Werte der Einstellung `SecondAction` sind dieselben wie die Werte der Einstellun `FirstAction`. Wenn als erste Aktion `Skip` oder `Remove` ausgewählt ist, muss keine zweite Aktion angegeben werden. In allen anderen Fällen wird empfohlen, zwei Aktionen anzugeben. Wenn Sie keine zweite Aktion angegeben haben, wendet die App `Skip` (überspringe als zweite Aktion an. Standardwert: `Skip`
`UseExcludeMasks`	Aktiviert den Ausschluss von Objekten, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, von der Untersuchung.	`Yes` – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, aus der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht aus der Untersuchur ausschließen.

`ExcludeMasks.item_#`	Ausschluss von der Untersuchung von Objekten nach Name oder Maske. Mit dieser Einstellung können Sie eine einzelne Datei anhand des Namens oder mehrere Dateien anhand von Masken im Shell-Format aus dem angegebenen Untersuchungsbereich ausschließen.
	
	Bevor Sie den Wert dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseExcludeMasks` aktiviert ist.
		Der Standardwert ist nicht angegeben.
		
		Beispiel:
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Aktiviert den Ausschluss von	`Yes` – Objekte, die Bedrohungen enthalter

	Objekten mit Bedrohungen, die durch die Einstellung `ExcludeThreats.item_#` festgelegt sind, von der Untersuchung.	die in der Einstellung `ExcludeThreats.item_#` angegeben sin von der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die Bedrohungen enthalten, die in der Einstellung `ExcludeThreats.item_#` angegeben sind, nicht von der Untersuchur ausschließen.

`ExcludeThreats.item_#`	Schließt Objekte nach dem Namen der in den Objekten gefundenen Bedrohungen von der Untersuchung aus. Bevor Sie die Werte dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseExcludeThreats` aktiviert ist.
	Um ein Objekt von der Untersuchung auszuschließen, geben Sie den vollständigen Namen der Bedrohung an, die im Objekt gefunden wurde, d. h. die Zeile mit der Entscheidung der App, dass dieses Objekt infiziert ist.
	Sie können beispielsweise ein Tool zum Sammeln von Informationen über Ihr Netzwerk verwenden. Damit es von der App nicht blockiert wird, fügen Sie den vollständigen Namen der darin enthaltenen Bedrohung zur Liste der Bedrohungen hinzu, die von der Untersuchung ausgenommen sind.
	Den vollständigen Namen der im Objekt gefundenen Bedrohung finden Sie im Protokoll der App oder auf der Website https://threats.kaspersky.com.
		Beim Wert der Einstellung muss die Groß- und Kleinschreibung beachtet werden.
		Der Standardwert ist nicht angegeben.
		Beispiel:
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Aktivieren der Verwendung von globalen Ausnahmen während der Untersuchung.	`Yes` (Standardwert) – Globale Ausnahmen verwenden. `No` – Keine globale Ausnahmen verwenden
`UseOASExclusions`	Aktivieren der Verwendung der Ausnahmen des Schutzes vor bedrohlichen Dateien während der Untersuchung.	`Yes` (Standardwert) – Ausnahmen des Schutzes vor bedrohlichen Dateien verwenden. `No` – Keine Ausnahmen des Schutzes vor bedrohlichen Dateien verwenden.
`ReportCleanObjects`	Aktiviert die Protokollierung von Informationen zu untersuchten Objekten, welche die App als nicht infiziert einstuft.	`Yes` – Informationen zu nicht infizierten Objekten im Protokoll speichern. `No` (Standardwert) – Informationen zu nicht infizierten Objekten nicht im Protokoll speichern.

	Sie können diese Einstellung aktivieren, um beispielsweise sicherzustellen, dass ein bestimmtes Objekt durch die App untersucht wurde.	
`ReportPackedObjects`	Aktiviert das Protokollieren von Informationen über untersuchte Objekte, die Bestandteil zusammengesetzter Objekte sind. Sie können diese Einstellung aktivieren, um beispielsweise sicherzustellen, dass ein bestimmtes Objekt innerhalb eines Archivs von der App untersucht wurde.	`Yes` – Informationen über die Untersuchur von Objekten, die zu einem Archiv gehören im Protokoll speichern. `No` (Standardwert) – Informationen über d Untersuchung von Objekten, die zu einem Archiv gehören, nicht im Protokoll speicher
`ReportUnprocessedObjects`	Aktiviert das Protokollieren von Informationen über Objekte, die aus einem bestimmten Grund nicht verarbeitet wurden.	`Yes` – Informationen zu nicht verarbeitete Objekten im Protokoll speichern. `No` (Standardwert) – Informationen zu nich verarbeiteten Objekten nicht im Protokoll speichern.
`UseAnalyzer`	Aktiviert die heuristische Analyse. Mithilfe der heuristischen Analyse kann die App Bedrohungen bereits erkennen, bevor sie den Virenanalysten bekannt sind.	`Yes` (Standardwert) – Heuristische Analys aktivieren. `No` – Heuristische Analyse deaktivieren.
`HeuristicLevel`	Legt die Stufe der heuristischen Analyse fest. Sie können die Ebene der heuristischen Analyse festlegen. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Gründlichkeit der Suche nach Bedrohungen, der Belastung der Betriebssystemressourcen und der Untersuchungsdauer. Je höher die festgelegte Ebene der heuristischen Analyse, desto mehr Ressourcen verbraucht die Untersuchung und desto länger dauert sie.	`Light` – Oberflächlichste Untersuchung m minimaler Belastung des Systems. `Medium` – Mittlere Ebene der heuristischer Analyse mit ausgeglichener Belastung des Betriebssystems. `Deep` – Gründlichste Untersuchung mit maximaler Belastung des Betriebssystems. `Recommended` (Standardwert) – Der empfohlene Wert.
`UseIChecker`	Aktiviert die Nutzung der iChecker-Technologie.	`Yes` (Standardwert) – Nutzung der iChecker-Technologie aktivieren. `No` – Nutzung der iChecker-Technologie deaktivieren.
`DeviceNameMasks.item_#`	Liste mit Namen der Geräte, deren Bootsektoren von der App untersucht werden.	`AllObjects` – Untersuchung der Bootsektoren aller Geräte.

	Der Einstellungswert darf nicht leer sein. Um die Aufgabe auszuführen, müssen Sie mindestens eine Maske für Gerätenamen angeben.	`<Maske für Gerätenamen>` – Untersuchung der Bootsektoren von den Geräten, deren Namen von der Maske eingeschlossen werden. Standardwert: `/**` (beliebiger Zeichensatz im Gerätenamen, einschließlich des Zeichen `/`)
Der Abschnitt **[ScanScope.item_#]** enthält die folgenden Parameter:		
`AreaDesc`	Beschreibung des Untersuchungsbereichs mit zusätzlichen Informationen über den Untersuchungsbereich. Die maximale Länge einer Zeichenfolge, die mit dieser Einstellung angegeben werden kann, beträgt 4096 Zeichen.	Standardwert: `All objects`. Beispiel: `AreaDesc="Mail bases scan"`
`UseScanArea`	Aktiviert die Untersuchung des angegebenen Bereichs. Um die Aufgabe auszuführen, müssen Sie mindestens einen zu untersuchenden Bereich angeben.	`Yes` (Standardwert) – Den angegebenen Bereich untersuchen. `No` – Angegebenen Bereich nicht untersuchen.
`AreaMask.item_#`	Einschränkung des Untersuchungsbereichs. Im Untersuchungsbereich untersucht die App nur Dateien, die mit Masken im Shell-Format angegeben wurden. Wenn die Einstellung nicht angegeben wurde, untersucht die App alle Objekte im Untersuchungsbereich. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: `*` (alle Objekte untersuchen Beispiel: `AreaMask.item_<Nummer des Elements>=*doc`
`Path`	Pfad zum Verzeichnis mit untersuchten Objekten.	`<Pfad zum lokalen Verzeichnis>` – Objekte im angegebenen Verzeichnis untersuchen. `Shared:NFS` – Ressourcen des Gerätedateisystems untersuchen, auf die über das NFS-Protokoll zugegriffen wird. `Shared:SMB` – Ressourcen des Gerätedateisystems untersuchen, auf die über das Samba-Protokoll zugegriffen wird `Mounted:NFS` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über NFS-Protokoll eingebunden sind. `Mounted:SMB` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über das Samba-Protokoll eingebunden sind. `AllRemoteMounted` – alle Remote-Verzeichnisse untersuchen, die auf dem Gerät über Samba- oder NFS-Protokolle gemountet sind.

		`AllShared` – Ressourcen des Gerätedateisystems untersuchen, auf die über das Samba- und NFS-Protokoll zugegriffen wird. `< Typ des Dateisystems >` – alle Ressourcen des angegebenen Dateisysten des Geräts untersuchen.
Der Abschnitt **[ExcludedFromScanScope.item_#]** enthält folgende Einstellungen:		
`AreaDesc`	Beschreibung des Ausschlussbereichs von der Untersuchung mit zusätzlichen Informationen über den Ausschlussbereich.	Der Standardwert ist nicht angegeben.
`UseScanArea`	Schließt den angegebenen Bereich von der Untersuchung aus.	`Yes` (Standardwert) – Den angegebenen Bereich ausschließen. `No` – Den angegebenen Bereich nicht ausschließen.
`AreaMask.item_#`	Einschränkung des von der Untersuchung ausgeschlossenen Bereichs. Im Ausschlussbereich schließt die App nur Dateien aus, die mittels Masken im Shell-Format angegeben wurden. Wenn die Einstellung nicht angegeben wurde, schließt die App alle Objekte im Ausschlussbereich aus. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: `*` (alle Objekte ausschließer
`Path`	Pfad zum Verzeichnis mit ausgeschlossenen Objekten.	`< Pfad zum lokalen Verzeichnis >` – Objekte im angegebenen Verzeichnis (und dessen Unterverzeichnissen) von der Untersuchung ausschließen. Bei der Angab des Pfades können Sie Masken verwenden

Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Bei Systemen mit dem Dateisystem BTRFS und aktivierten aktiven Snapshots wird es zur Optimierung der Untersuchungsaufgaben empfohlen, den Pfad mit dem im "Read only"-Modus gemounteten Snapshots den Ausschlüsse hinzuzufügen. Beispielsweise können in Systemen auf Basis von SUSE/OpenSUSE eines Ausschluss folgendermaßen angeben `/.snapshots/*/snapshot/`.

`Mounted:NFS` – Remote-Verzeichnisse, di auf dem Gerät über das NFS-Protokoll gemountet sind, von der Untersuchung ausschließen.

`Mounted:SMB` – Remote-Verzeichnisse, di auf dem Gerät über das Samba-Protokoll gemountet sind, von der Untersuchung ausschließen.

`AllRemoteMounted` – Alle Remote-Verzeichnisse, die auf dem Gerät über Samba- oder NFS-Protokolle gemountet sind, von der Untersuchung ausschließen.

`< Typ des Dateisystems >` – alle Ressourcen des angegebenen Dateisysten des Geräts von der Untersuchung ausschließen.

		Remote-Verzeichnisse werden nur dann von der Untersuchung durch die App ausgeschlossen, wenn sie bereits vor dem Aufgabenstart eingebunden wurden. Remote-Verzeichnisse, die erst nach dem Aufgabenstart eingebunden wurden, werden von der Untersuchung nicht ausgeschlossen.

Benutzerdefinierte Untersuchung von Dateien und Verzeichnissen

Mit dem Befehl `kesl-control --scan-file` können Sie eine benutzerdefinierte Untersuchung bestimmter Dateien und Verzeichnisse durchführen.

Eine benutzerdefinierte Untersuchung wird mit Einstellungen durchgeführt, die in der vordefinierten Aufgabe *Scan_File* (ID:3) gespeichert sind. Sie können die Einstellungen für die benutzerdefinierte Dateiuntersuchung konfigurieren, indem Sie die Einstellungen dieser Aufgabe ändern (siehe Tabelle unten).

Um eine benutzerdefinierte Untersuchung der angegebenen Dateien und Verzeichnisse durchzuführen, führen Sie den folgenden Befehl aus:

```
kesl-control --scan-file <Pfad> [--action <Aktion>]
```

Wobei gilt:

- `<Pfad>` – Pfad zu der Datei oder dem Verzeichnis, die Sie überprüfen möchten. Sie können mehrere, durch Leerzeichen getrennte Pfade angeben.
- `--action <Aktion>` – Aktion, welche die App für infizierte Objekte ausführen soll. Wenn Sie den Schalter `--action` nicht angeben, führt die App die empfohlene Aktion aus.

Als Ergebnis der Ausführung des Befehls wird eine temporäre Aufgabe zur Untersuchung von Dateien erstellt, die nach Abschluss automatisch gelöscht wird. Gleichzeitig werden die Ergebnisse der Untersuchung in die Konsole ausgegeben.

Die Tabelle beschreibt alle verfügbaren Werte und Standardwerte aller Einstellungen, die Sie für die Aufgabe *Scan_File* angeben können.

Die in der Aufgabe `Scan_File` angegebenen Abschnitte `[ScanScope.item_#]` und *[ExcludedFromScanScope.item_#]* werden bei der Durchführung einer benutzerdefinierten Untersuchung nicht berücksichtigt.

Einstellungen der Aufgabe Scan_File

Einstellung	Beschreibung	Werte
`ScanFiles`	Aktiviert die Untersuchung von Dateien.	`Yes` (Standardwert) – Dateien untersuche `No` – Dateien nicht untersuchen.
`ScanBootSectors`	Aktiviert die Untersuchung der Bootsektoren.	`Yes` – Bootsektoren untersuchen.

		`No` (Standardwert) – Bootsektoren nicht untersuchen.
`ScanComputerMemory`	Aktiviert die Untersuchung des Prozess- und Kernelspeichers.	`Yes` – Prozess-Speicher und Kernelspeich untersuchen. `No` (Standardwert) – Prozess-Speicher un Kernelspeicher nicht .untersuchen
`ScanStartupObjects`	Aktiviert die Untersuchung der Autostart-Objekte.	`Yes` – Autostart-Objekte untersuchen. `No` (Standardwert) – Autostart-Objekte nicht untersuchen.
`ScanArchived`	Aktiviert die Untersuchung von Archiven (einschließlich selbstentpackender sfx-Archive). Die App untersucht Archive wie .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Die Liste der unterstützten Archivformate hängt von den verwendeten App-Datenbanken ab.	`Yes` (Standardwert) – Archive untersuche Wenn der Wert `FirstAction=Recommended` angegeben ist, löscht die App je nach Archivtyp entweder das infizierte Objekt oder das gesamte Archiv, das die Bedrohung enthält `No` – Archive nicht untersuchen.
`ScanSfxArchived`	Aktiviert die Untersuchung von nur selbstentpackenden Archiven (Archiven, zu deren Bestandteilen ein ausführbares Dekompressionsmodul gehört).	`Yes` (Standardwert) – Selbstentpackende Archive untersuchen. `No` – Selbstentpackende Archive nicht untersuchen.
`ScanMailBases`	Aktiviert die Untersuchung von E-Mail-Datenbanken von Microsoft Outlook, Outlook Express, The Bat! und anderen Mail-Clients.	`Yes` – Dateien von E-Mail-Datenbanken untersuchen. `No` (Standardwert) – Dateien von E-Mail-Datenbanken nicht untersuchen.
`ScanPlainMail`	Aktiviert die Untersuchung von E-Mail-Nachrichten im Textformat (plain text).	`Yes` – E-Mail-Nachrichten im Textformat untersuchen. `No` (Standardwert) – E-Mail-Nachrichten ir Textformat nicht untersuchen.
`SizeLimit`	Maximale Größe des zu untersuchenden Objekts (in Megabyte). Wenn die Größe des zu untersuchenden Objekts den angegebenen Wert überschreitet, überspringt die App das Objekt während der Untersuchung.	0 – 999999 0 – Die App untersucht Objekte beliebiger Größe. Standardwert: 0.
`TimeLimit`	Maximale Untersuchungsdauer (in Sekunden) eines Objekts. Die App stellt die Untersuchung eines Objekts ein, wenn sie länger dauert als durch diese Einstellung festgelegt.	0 – 9999 0 – die Untersuchungsdauer für Objekte is nicht begrenzt. Standardwert: 0.
`FirstAction`	Auswahl der ersten Aktion, welche die App für infizierte Objekte ausführen soll.	`Disinfect` (desinfizieren) – Die App versucht, ein Objekt zu desinfizieren, und speichert eine Kopie davon im Backup-Speicher. Wenn die Desinfektion fehlschläg

		(beispielsweise, weil der Typ des Objekts oder der Typ der Bedrohung im Objekt nicht desinfiziert werden kann), belässt die App das Objekt unverändert. Wenn die erste Aktion auf `Desinfizieren` festgelegt ist, wird empfohlen, die zweite Aktion mithilfe der Einstellung `SecondAction` anzugeben `Remove` (löschen) – Die App löscht das infizierte Objekt, nachdem eine Backup-Kopie davon erstellt wurde. `Recommended` (empfohlene Aktion ausführen) – Die App wählt automatisch eine Aktion für das Objekt und führt sie au wobei Informationen zu der im Objekt gefundenen Bedrohung berücksichtigt werden. Beispielsweise löscht Kaspersky Endpoint Security Trojaner sofort, da sie andere Dateien nicht infizieren und deshalb keine Desinfektion erfordern. `Skip` (überspringen) – Die App unternimm keinen Versuch, das infizierte Objekt zu desinfizieren oder zu löschen. Informatione über das infizierte Objekt werden im Protokoll gespeichert. Standardwert: `Recommended`
`SecondAction`	Auswahl der zweiten Aktion, welche die App für infizierte Objekte ausführen soll. Die App führt die zweite Aktion aus, wenn die Ausführung der ersten Aktion misslingt.	Die Werte der Einstellung `SecondAction` sind dieselben wie die Werte der Einstellun `FirstAction`. Wenn als erste Aktion `Skip` oder `Remove` ausgewählt ist, muss keine zweite Aktion angegeben werden. In allen anderen Fällen wird empfohlen, zwei Aktionen anzugeben. Wenn Sie keine zweite Aktion angegeben haben, wendet die App `Skip` (überspringe als zweite Aktion an. Standardwert: `Skip`
`UseExcludeMasks`	Aktiviert den Ausschluss von Objekten, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, von der Untersuchung.	`Yes` – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, aus der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht aus der Untersuchur ausschließen.

`ExcludeMasks.item_#`	Ausschluss von der Untersuchung von Objekten nach Name oder Maske. Mit dieser Einstellung können Sie eine einzelne Datei anhand des Namens oder mehrere Dateien anhand von Masken im Shell-Format aus dem angegebenen Untersuchungsbereich ausschließen.	Der Standardwert ist nicht angegeben.
		
		Beispiel:
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Aktiviert den Ausschluss von	`Yes` – Objekte, die Bedrohungen enthalter

	Objekten mit Bedrohungen, die durch die Einstellung `ExcludeThreats.item_#` festgelegt sind, von der Untersuchung.	die in der Einstellung `ExcludeThreats.item_#` angegeben sin von der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die Bedrohungen enthalten, die in der Einstellung `ExcludeThreats.item_#` angegeben sind, nicht von der Untersuchur ausschließen.

`ExcludeThreats.item_#`	Schließt Objekte nach dem Namen der in den Objekten gefundenen Bedrohungen von der Untersuchung aus. Bevor Sie die Werte dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseExcludeThreats` aktiviert ist.
	Um ein Objekt von der Untersuchung auszuschließen, geben Sie den vollständigen Namen der Bedrohung an, die im Objekt gefunden wurde, d. h. die Zeile mit der Entscheidung der App, dass dieses Objekt infiziert ist.
	Sie können beispielsweise ein Tool zum Sammeln von Informationen über Ihr Netzwerk verwenden. Damit es von der App nicht blockiert wird, fügen Sie den vollständigen Namen der darin enthaltenen Bedrohung zur Liste der Bedrohungen hinzu, die von der Untersuchung ausgenommen sind.
	Den vollständigen Namen der im Objekt gefundenen Bedrohung finden Sie im Protokoll der App oder auf der Website https://threats.kaspersky.com.
		Beim Wert der Einstellung muss die Groß- und Kleinschreibung beachtet werden.
		Der Standardwert ist nicht angegeben.
		Beispiel:
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Aktivieren der Verwendung von globalen Ausnahmen während der Untersuchung.	`Yes` (Standardwert) – Globale Ausnahmen verwenden. `No` – Keine globale Ausnahmen verwenden
`UseOASExclusions`	Aktivieren der Verwendung der Ausnahmen des Schutzes vor bedrohlichen Dateien während der Untersuchung.	`Yes` (Standardwert) – Ausnahmen des Schutzes vor bedrohlichen Dateien verwenden. `No` – Keine Ausnahmen des Schutzes vor bedrohlichen Dateien verwenden.
`ReportCleanObjects`	Aktiviert die Protokollierung von Informationen zu untersuchten Objekten, welche die App als nicht infiziert einstuft.	`Yes` – Informationen zu nicht infizierten Objekten im Protokoll speichern. `No` (Standardwert) – Informationen zu nich infizierten Objekten nicht im Protokoll speichern.

	Sie können diese Einstellung aktivieren, um beispielsweise sicherzustellen, dass ein bestimmtes Objekt durch die App untersucht wurde.	
`ReportPackedObjects`	Aktiviert das Protokollieren von Informationen über untersuchte Objekte, die Bestandteil zusammengesetzter Objekte sind. Sie können diese Einstellung aktivieren, um beispielsweise sicherzustellen, dass ein bestimmtes Objekt innerhalb eines Archivs von der App untersucht wurde.	`Yes` – Informationen über die Untersuchur von Objekten, die zu einem Archiv gehören im Protokoll speichern. `No` (Standardwert) – Informationen über d Untersuchung von Objekten, die zu einem Archiv gehören, nicht im Protokoll speicher
`ReportUnprocessedObjects`	Aktiviert das Protokollieren von Informationen über Objekte, die aus einem bestimmten Grund nicht verarbeitet wurden.	`Yes` – Informationen zu nicht verarbeitete Objekten im Protokoll speichern. `No` (Standardwert) – Informationen zu nich verarbeiteten Objekten nicht im Protokoll speichern.
`UseAnalyzer`	Aktiviert die heuristische Analyse. Mithilfe der heuristischen Analyse kann die App Bedrohungen bereits erkennen, bevor sie den Virenanalysten bekannt sind.	`Yes` (Standardwert) – Heuristische Analys aktivieren. `No` – Heuristische Analyse deaktivieren.
`HeuristicLevel`	Legt die Stufe der heuristischen Analyse fest. Sie können die Ebene der heuristischen Analyse festlegen. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Gründlichkeit der Suche nach Bedrohungen, der Belastung der Betriebssystemressourcen und der Untersuchungsdauer. Je höher die festgelegte Ebene der heuristischen Analyse, desto mehr Ressourcen verbraucht die Untersuchung und desto länger dauert sie.	`Light` – Oberflächlichste Untersuchung m minimaler Belastung des Systems. `Medium` – Mittlere Ebene der heuristischer Analyse mit ausgeglichener Belastung des Betriebssystems. `Deep` – Gründlichste Untersuchung mit maximaler Belastung des Betriebssystems. `Recommended` (Standardwert) – Der empfohlene Wert.
`UseIChecker`	Aktiviert die Nutzung der iChecker-Technologie.	`Yes` (Standardwert) – Nutzung der iChecker-Technologie aktivieren. `No` – Nutzung der iChecker-Technologie deaktivieren.
`DeviceNameMasks.item_#`	Liste mit Namen der Geräte, deren Bootsektoren von der App untersucht werden.	`AllObjects` – Untersuchung der Bootsektoren aller Geräte.

	Der Einstellungswert darf nicht leer sein. Um die Aufgabe auszuführen, müssen Sie mindestens eine Maske für Gerätenamen angeben.	`<Maske für Gerätenamen>` – Untersuchung der Bootsektoren von den Geräten, deren Namen von der Maske eingeschlossen werden. Standardwert: `/**` (beliebiger Zeichensatz im Gerätenamen, einschließlich des Zeichen `/`)
Der Abschnitt **[ScanScope.item_#]** enthält die folgenden Parameter:		
`AreaDesc`	Beschreibung des Untersuchungsbereichs mit zusätzlichen Informationen über den Untersuchungsbereich. Die maximale Länge einer Zeichenfolge, die mit dieser Einstellung angegeben werden kann, beträgt 4096 Zeichen.	Standardwert: `All objects`. Beispiel: `AreaDesc="Mail-Datenbanken untersuchen"`
`UseScanArea`	Aktiviert die Untersuchung des angegebenen Bereichs. Um die Aufgabe auszuführen, müssen Sie mindestens einen zu untersuchenden Bereich angeben.	`Yes` (Standardwert) – Den angegebenen Bereich untersuchen. `No` – Angegebenen Bereich nicht untersuchen.
`AreaMask.item_#`	Einschränkung des Untersuchungsbereichs. Im Untersuchungsbereich untersucht die App nur Dateien, die mit Masken im Shell-Format angegeben wurden. Wenn die Einstellung nicht angegeben wurde, untersucht die App alle Objekte im Untersuchungsbereich. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: `*` (alle Objekte untersuchen Beispiel: `AreaMask.item_<Nummer des Elements>=*doc`
`Path`	Pfad zum Verzeichnis mit untersuchten Objekten.	`<Pfad zum lokalen Verzeichnis>` – Objekte im angegebenen Verzeichnis untersuchen. `Shared:NFS` – Ressourcen des Gerätedateisystems untersuchen, auf die über das NFS-Protokoll zugegriffen wird. `Shared:SMB` – Ressourcen des Gerätedateisystems untersuchen, auf die über das Samba-Protokoll zugegriffen wird `Mounted:NFS` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über NFS-Protokoll eingebunden sind. `Mounted:SMB` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über das Samba-Protokoll eingebunden sind. `AllRemoteMounted` – alle Remote-Verzeichnisse untersuchen, die auf dem Gerät über Samba- oder NFS-Protokolle gemountet sind.

		`AllShared` – Ressourcen des Gerätedateisystems untersuchen, auf die über das Samba- und NFS-Protokoll zugegriffen wird. `< Typ des Dateisystems >` – alle Ressourcen des angegebenen Dateisysten des Geräts untersuchen.
Der Abschnitt **[ExcludedFromScanScope.item_#]** enthält die folgenden Parameter:		
`AreaDesc`	Beschreibung des Ausschlussbereichs von der Untersuchung mit zusätzlichen Informationen über den Ausschlussbereich.	Der Standardwert ist nicht angegeben.
`UseScanArea`	Schließt den angegebenen Bereich von der Untersuchung aus.	`Yes` (Standardwert) – Den angegebenen Bereich ausschließen. `No` – Den angegebenen Bereich nicht ausschließen.
`AreaMask.item_#`	Einschränkung des von der Untersuchung ausgeschlossenen Bereichs. Im Ausschlussbereich schließt die App nur Dateien aus, die mittels Masken im Shell-Format angegeben wurden. Wenn die Einstellung nicht angegeben wurde, schließt die App alle Objekte im Ausschlussbereich aus. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: * (alle Objekte ausschließer
`Path`	Pfad zum Verzeichnis mit ausgeschlossenen Objekten.	`< Pfad zum lokalen Verzeichnis >` – Objekte im angegebenen Verzeichnis (und dessen Unterverzeichnissen) von der Untersuchung ausschließen. Bei der Angab des Pfades können Sie Masken verwenden

Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Bei Systemen mit dem Dateisystem BTRFS und aktivierten aktiven Snapshots wird es zur Optimierung der Untersuchungsaufgaben empfohlen, den Pfad mit dem im "Read only"-Modus gemounteten Snapshots den Ausschlüsse hinzuzufügen. Beispielsweise können in Systemen auf Basis von SUSE/OpenSUSE eines Ausschluss folgendermaßen angeben `/.snapshots/*/snapshot/`.

`Mounted:NFS` – Remote-Verzeichnisse, di auf dem Gerät über das NFS-Protokoll gemountet sind, von der Untersuchung ausschließen.

`Mounted:SMB` – Remote-Verzeichnisse, di auf dem Gerät über das Samba-Protokoll gemountet sind, von der Untersuchung ausschließen.

`AllRemoteMounted` – Alle Remote-Verzeichnisse, die auf dem Gerät über Samba- oder NFS-Protokolle gemountet sind, von der Untersuchung ausschließen.

`< Typ des Dateisystems >` – alle Ressourcen des angegebenen Dateisysten des Geräts von der Untersuchung ausschließen.

		Remote-Verzeichnisse werden nur dann von der Untersuchung durch die App ausgeschlossen, wenn sie bereits vor dem Aufgabenstart eingebunden wurden. Remote-Verzeichnisse, die erst nach dem Aufgabenstart eingebunden wurden, werden von der Untersuchung nicht ausgeschlossen.

Untersuchung wichtiger Bereiche

Während der Untersuchung wichtiger Bereiche kann Kaspersky Endpoint Security Bootsektoren, Autostart-Objekte, Prozess- und Kernelspeicher untersuchen.

Wenn Schadsoftware entdeckt wird, kann die App die infizierte Datei löschen und den von dieser Datei gestarteten schädlichen Prozess beenden.

So können Sie eine Untersuchung wichtiger Bereiche durchführen und Untersuchungseinstellungen konfigurieren:

- Wählen Sie die zu untersuchenden Betriebssystemobjekte aus. Standardmäßig ist die Untersuchung von Bootsektoren, Prozess- und Kernelspeicher, Autostart-Objekten und Archiven aktiviert. Bei der Untersuchung wichtiger Bereiche werden Dateien standardmäßig nicht untersucht.
- Begrenzen Sie die Größe des untersuchten Objekts und die Untersuchungsdauer für das Objekt.
- Wählen Sie die Aktionen aus, welche die App für infizierte Objekte ausführen soll.
- Konfigurieren Sie den Ausschluss von Objekten von der Untersuchung nach:
  - Namen oder Masken
  - Namen der in den Objekten gefundenen Bedrohungen
- Aktivieren oder deaktivieren Sie für die Untersuchungen die Verwendung von globalen Ausnahmen und von Ausnahmen des Schutzes vor bedrohlichen Dateien.
- Aktivieren Sie die Protokollierung von Informationen zu untersuchten nicht infizierten Objekten, zu untersuchten Objekten in Archiven und zu nicht verarbeiteten Objekten.
- Konfigurieren Sie die Verwendung der heuristischen Analyse und der iChecker-Technologie während der Untersuchung.
- Beschränken Sie die Anzahl der Geräte, deren Bootsektoren untersucht werden müssen.
- Konfigurieren Sie Untersuchungsbereiche und von der Untersuchung auszuschließende Bereiche.

Untersuchung wichtiger Bereiche in der Web Console

In der Web Console können Sie mithilfe der Aufgabe *Untersuchung wichtiger Bereiche* wichtige Bereiche des Betriebssystems des geschützten Geräts untersuchen.

Sie können Benutzeraufgaben zur Untersuchung wichtiger Bereiche erstellen und starten. Sie können die Untersuchungseinstellungen konfigurieren, indem Sie die Aufgabeneinstellungen ändern.

Einstellungen der Aufgabe zur Untersuchung wichtiger Bereiche

Einstellung	Beschreibung
Archive untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Archiven. Wenn das Kontrollkästchen aktiviert ist, so untersucht die App Archive.

	Um ein Archiv zu untersuchen, muss es zunächst von der App entpackt werden, was die Untersuchung verlangsamen kann. Sie können die Dauer der Untersuchung von Archiven reduzieren, indem Sie im Abschnitt **Allgemeine Untersuchungseinstellungen** die Einstellungen **Dateien überspringen, deren Untersuchung länger dauert als (Sek.)** und/oder **Dateien überspringen, die größer sind als (MB)** konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Archive. Das Kontrollkästchen ist standardmäßig aktiviert.
Selbstentpackende Archive untersuchen	Das Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung *selbstentpackender Archive (self-extracting archives)*. Selbstentpackende Archive sind Archive, die ein ausführbares Modul zum Entpacken enthalten. Wenn das Kontrollkästchen aktiviert ist, untersucht die App selbstentpackende Archive. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine selbstentpackenden Dateien. Dieses Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Archive untersuchen** deaktiviert ist. Das Kontrollkästchen ist standardmäßig aktiviert.
Mail-Datenbanken untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Mail-Datenbanken der Anwendungen Microsoft Outlook, Outlook Express, The Bat! und anderen E-Mail-Clients. Wenn das Kontrollkästchen aktiviert ist, untersucht die App die Dateien von Mail-Datenbanken. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Dateien von Mail-Datenbanken. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Dateien in Mail-Formaten untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Dateien von E-Mail-Nachrichten im Textformat (plain text). Wenn das Kontrollkästchen aktiviert ist, untersucht die App E-Mail-Nachrichten im Textformat. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App E-Mail-Nachrichten im Textformat nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Dateien überspringen, deren Untersuchung länger dauert als (Sek.)	In diesem Feld können Sie die erlaubte Höchstdauer für die Untersuchung der Datei in Sekunden angeben. Nach Ablauf des angegebenen Zeitraums bricht die App die Untersuchung der Datei ab. Zulässige Werte: 0–9999. Ist der Wert 0 angegeben, dann ist die Untersuchungsdauer nicht beschränkt. Standardwert: 0.
Dateien überspringen, die größer sind als (MB)	In diesem Feld können Sie die maximale Größe der untersuchten Datei in Megabyte angeben. Zulässige Werte: 0–999999. Ist der Wert 0 angegeben, untersucht die App Dateien jeder Größe. Standardwert: 0.
Virenfreie Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectProcessed*. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt.

	Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Nicht verarbeitete Dateien protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectNotProcessed*, wenn eine Datei während der Untersuchung nicht verarbeitet werden kann. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *ObjectNotProcessed*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *ObjectNotProcessed*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Gepackte Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *PackedObjectDetected* für alle erkannten gepackten Objekte. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *PackedObjectDetected*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *PackedObjectDetected*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
iChecker-Technologie verwenden	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung nur neuer oder seit der letzten Untersuchung geänderter Dateien. Wenn das Kontrollkästchen aktiviert ist, untersucht die App nur neue oder seit der letzten Untersuchung geänderte Dateien. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App Dateien unabhängig von ihrem Erstellungs- oder Änderungsdatum. Das Kontrollkästchen ist standardmäßig aktiviert.
Heuristische Analyse verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die heuristische Analyse bei der Untersuchung von Dateien. Das Kontrollkästchen ist standardmäßig aktiviert.
Stufe der heuristischen Analyse	Wenn das Kontrollkästchen **Heuristische Analyse verwenden** aktiviert ist, können Sie die Ebene der heuristischen Analyse in der Dropdown-Liste festlegen: • **Oberflächlich** – Die am wenigsten detaillierte Untersuchung, minimale Systembelastung. • **Mittel** – Mittlere Untersuchung, ausgeglichene Systembelastung. • **Tief** – Detaillierteste Untersuchung, maximale Systembelastung. • **Empfohlen** (Standardwert) – Optimale Stufe, die von den Kaspersky-Experten empfohlen wird. Sie bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Geräte.
Erste Aktion	In der Dropdown-Liste können Sie die erste Aktion auswählen, die von der App für das gefundene infizierte Objekt ausgeführt werden soll: • Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt.

	• Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Informationen zur Gefahrenstufe der in der Datei erkannten Bedrohung und zur Möglichkeit ihrer Desinfektion (Standardwert). • Objekt **überspringen**.
Zweite Aktion	In dieser Dropdown-Liste können Sie die zweite Aktion auswählen, die von der App für ein infiziertes Objekt ausgeführt werden soll, falls die erste Aktion nicht erfolgreich war: • Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Daten zur in der Datei erkannten Gefahrenstufe der Bedrohung und zur Möglichkeit ihrer Desinfektion. • Objekt **überspringen** (Standardwert).
Untersuchungsbereiche	Eine Tabelle mit Bereichen, die von der Aufgabe untersucht werden sollen. Standardmäßig enthält die Tabelle einen Untersuchungsbereich, der alle Verzeichnisse des lokalen Dateisystems umfasst. Sie können Untersuchungsbereiche in der Tabelle hinzufügen, konfigurieren, löschen, nach oben verschieben und nach unten verschieben. Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten. Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren. Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde. Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben. Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren. Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Ein Klick auf den Namen des Untersuchungsbereichs öffnet das Fenster **<Name des Untersuchungsbereichs>**. In diesem Fenster können Sie die Einstellungen des ausgewählten Untersuchungsbereichs ändern.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **<Neuer Untersuchungsbereich>**. In diesem Fenster können Sie einen neuen Untersuchungsbereich festlegen.

Fenster zum Hinzufügen des Untersuchungsbereichs

In diesem Fenster können Sie einen neuen Untersuchungsbereich hinzufügen oder anpassen.

Einstellungen des Untersuchungsbereichs

Einstellung	Beschreibung
Name des Bereichs	Eingabefeld für den Namen der Untersuchungsbereichs. Dieser Name wird in der Tabelle **Untersuchungsbereiche** im Abschnitt **Untersuchungseinstellungen** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung dieses Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, verarbeitet die App diesen Untersuchungsbereich während ihrer Ausführung. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die App diesen Untersuchungsbereich während ihrer Ausführung nicht. Sie können diesen Bereich zu einem späteren Zeitpunkt zu den Betriebseinstellungen der Komponente hinzufügen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	In der Dropdown-Liste können Sie den Typ des Dateisystems auswählen: • **Lokal** (Standardwert) – Lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie den Pfad zu einem lokalen Verzeichnis angeben. • **Mounted** – Gemountete Remote-Verzeichnisse oder lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie das Protokoll oder den Namen des Dateisystems angeben. • **Freigegeben** – Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind.

	• **Alle freigegebenen** – Alle Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind.
Zugriffsprotokoll	In der Dropdown-Liste können Sie das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind. Diese Dropdown-Liste ist verfügbar, wenn in der Dropdown-Liste für Dateisysteme als Typ **Freigegeben** oder **Mounted** ausgewählt ist.
Pfad	Eingabefeld für den Pfad des Verzeichnisses, das in den Untersuchungsbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken und Tags verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

	Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardmäßige Pfadangabe **/** – Die App untersucht alle Verzeichnisse des lokalen Dateisystems. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Lokal** ausgewählt ist. Wenn in der Dropdown-Liste der Dateisysteme als Typ **Lokal** ausgewählt ist und kein Pfad angegeben wird, untersucht die App alle Verzeichnisse des lokalen Dateisystems.
Name der freigegebenen Ressource	Eingabefeld für den Namen der freigegebenen Ressource des Dateisystems, auf der sich die Verzeichnisse befinden, die Sie zum Untersuchungsbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste **Zugriffsprotokoll** das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der App während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster. Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Abschnitt "Untersuchungsbereiche"

Einstellungen des Untersuchungsbereichs der Aufgabe zur Untersuchung wichtiger Bereiche

Einstellung	Beschreibung
Dateien untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Dateien. Wenn das Kontrollkästchen aktiviert ist, untersucht die App Dateien. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Dateien. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Bootsektoren untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Bootsektoren. Wenn das Kontrollkästchen aktiviert ist, untersucht die App Bootsektoren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Bootsektoren. Das Kontrollkästchen ist standardmäßig aktiviert.
Kernelspeicher und gestartete Prozesse untersuchen.	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung des Arbeitsspeichers des Client-Geräts. Wenn diese Option aktiviert ist, überprüft die App den Kernel-Speicher und die gestarteten Prozesse. Wenn das Kontrollkästchen deaktiviert ist, überprüft die App den Kernel-Speicher und die gestarteten Prozesse nicht. Das Kontrollkästchen ist standardmäßig aktiviert.
Autostart-Objekte untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Autostart-Objekten. Wenn das Kontrollkästchen aktiviert ist, untersucht die App Autostart-Objekte. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Autostart-Objekte. Das Kontrollkästchen ist standardmäßig aktiviert.
Zu untersuchende Geräte	Der Link **Gerätemasken** anpassen öffnet das Fenster **Untersuchungsbereiche**. In diesem Fenster können Sie die Geräte angeben, deren Bootsektoren untersucht werden sollen.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält die Masken der Gerätenamen, deren Bootsektoren die App untersuchen soll. Standardmäßig enthält die Tabelle die Gerätenamen-Maske **/**** (alle Geräte).

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Abschnitt "Ausschlussbereiche"

Im Abschnitt **Ausschlussbereiche** der Aufgabe "Untersuchung wichtiger Bereiche" können Sie die Ausschlussbereiche, die Ausschlüsse nach Maske und Bedrohungsname sowie die Verwendung globaler Ausschlüsse und Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der Ausführung der Aufgabe konfigurieren.

Einstellungen der Ausschlüsse von der Untersuchung

Einstellung	Beschreibung
Ausschlussbereich anpassen	Der Link **Ausschlussbereiche anpassen** öffnet das Fenster **Ausschlussbereiche**. In diesem Fenster können Sie eine Liste mit Ausschlüsse von der Untersuchung festlegen.
Ausschlüsse nach Maske anpassen	Der Link **Ausschlüsse nach Maske anpassen** öffnet das Fenster **Ausschlüsse nach Maske**. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren.
Ausschlüsse nach Bedrohungsname anpassen	Der Link **Ausschlüsse nach Bedrohungsname anpassen** öffnet das Fenster **Ausschlüsse nach Bedrohungsname**. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren.
Globale Ausnahmen verwenden	Das Kontrollkästchen aktiviert oder deaktiviert den Ausschluss von in den globalen Ausnahmen angegeben Mountpunkten während der App-Ausführung. Wenn diese Option aktiviert ist, schließt die App die konfigurierten Mountpunkte von der Untersuchung aus. Das Kontrollkästchen ist standardmäßig aktiviert.
Ausschlüsse aus dem Schutz vor bedrohlichen Dateien verwenden	Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung konfigurierter Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der App-Ausführung. Wenn das Kontrollkästchen aktiviert ist, schließt die App jene Objekte von der Untersuchung aus, die in den Ausschlüssen der Komponente "Schutz vor bedrohlichen Dateien" angegeben sind. Das Kontrollkästchen ist standardmäßig aktiviert.

Fenster "Ausschlussbereiche"

Die Tabelle enthält Bereiche mit Ausschlüsse von der Untersuchung. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung

Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der App angewendet wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster zum Hinzufügen des Ausschlussbereichs

In diesem Fenster können Sie einen neuen Ausschlussbereich hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster **Ausschlussbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss des Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, wird dieser Bereich während der Ausführung der App von der Untersuchung oder vom Schutz ausgeschlossen. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich während der Ausführung der App in die Untersuchung oder den Schutz eingeschlossen. Im Folgenden können Sie diesen Bereich von der Untersuchung oder dem Schutz ausschließen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	In der Dropdown-Liste können Sie den Typ des Dateisystems auswählen, auf dem sich die Verzeichnisse befinden, die Sie zu den Ausschlüssen von der Untersuchung hinzufügen möchten: • **Lokal** – Lokale Verzeichnisse. • **Mounted** – Remote-Verzeichnisse, die auf dem Gerät eingebunden sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind.

Zugriffsprotokoll	In der Dropdown-Liste können Sie das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind. Diese Dropdown-Liste ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** ausgewählt ist.
Pfad	Eingabefeld für den Pfad des Verzeichnisses, das in den Ausschlussbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken und Tags verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

	Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Als Pfad ist standardmäßig **/** angegeben: Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Lokal** ausgewählt ist.
Name der freigegebenen Ressource	Eingabefeld für den Namen der freigegebenen Ressource des Dateisystems, auf der sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten: Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste **Zugriffsprotokoll** das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Untersuchung ausgeschlossen werden. Die Masken werden nur innerhalb des Verzeichnisses übernommen, das im Eingabefeld **Pfad** angegeben ist. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen. Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist. Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Maske"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren. Die App untersucht keine Dateien, deren Namen die angegebenen Masken enthalten. Standardmäßig ist die Liste mit Masken leer.

Sie können Masken hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist.

Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Bedrohungsname"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren. Die App blockiert die angegebenen Bedrohungen nicht. Standardmäßig ist die Liste mit den Namen von Bedrohungen leer.

Sie können Namen von Bedrohungen hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Bedrohung aus den Ausschlüsse.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens ein Bedrohungsname ausgewählt ist.

Ein Klick auf den Namen einer Bedrohung in der Tabelle öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung ändern, die von der Untersuchung ausgenommen wird.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung angeben, die von der Untersuchung ausgenommen wird.

Untersuchung wichtiger Bereiche in der Verwaltungskonsole

In der Verwaltungskonsole können Sie mithilfe der Aufgabe *Untersuchung wichtiger Bereiche* wichtige Bereiche des Betriebssystems des geschützten Geräts untersuchen.

Sie können Benutzeraufgaben zur Untersuchung wichtiger Bereiche erstellen und starten. Sie können die Untersuchungseinstellungen konfigurieren, indem Sie die Aufgabeneinstellungen ändern.

Im Abschnitt **Einstellungen** in den Eigenschaften der Aufgabe "Untersuchung wichtiger Bereiche" können Sie die in der folgenden Tabelle aufgeführten Einstellungen konfigurieren.

Einstellungen der Aufgabe zur Untersuchung wichtiger Bereiche

Einstellung	Beschreibung
Untersuchung	Diese Einstellungsgruppe enthält Schaltflächen, mit denen Fenster geöffnet werden können, in denen Sie die Untersuchungsbereiche, die Einstellungen des Untersuchungsbereichs und die Untersuchungseinstellungen anpassen können.
Aktion beim Erkennen einer Bedrohung	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, mit der das Fenster **Aktion beim Erkennen von Bedrohungen** geöffnet werden kann. In diesem Fenster können Sie die Aktionen konfigurieren, die von der App für das erkannte infizierte Objekt ausgeführt werden soll.

Im Abschnitt **Ausnahmen** in den Einstellungen der Aufgabe Aufgabe zur Untersuchung wichtiger Bereiche können Sie Ausschlussbereiche, Ausschlüsse nach Maske und Ausschlüsse nach Bedrohungsname anpassen.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält den Untersuchungsbereich. Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle einen Untersuchungsbereich, der alle Verzeichnisse des lokalen Dateisystems umfasst.

Einstellungen des Untersuchungsbereichs

Einstellung	Beschreibung
Name des Bereichs	Name des Untersuchungsbereichs

Pfad	Der Pfad zu dem zu untersuchenden Verzeichnis.
Status	Der Status gibt an, ob die App diesen Bereich während ihrer Ausführung untersucht.

Sie können Elemente in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.

Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Liste der Bereiche angeben sind. Um bei Bedarf für das Unterverzeichnis andere Sicherheitseinstellungen festzulegen als für das übergeordnete Verzeichnis, platzieren Sie erforderlichenfalls das Unterverzeichnis in der Liste über dem übergeordneten Verzeichnis.

Fenster "<Neuer Untersuchungsbereich>"

In diesem Fenster können Sie einen neuen Untersuchungsbereich hinzufügen oder anpassen.

Einstellungen des Untersuchungsbereichs

Einstellung	Beschreibung
Name des Untersuchungsbereichs	Eingabefeld für den Namen der Untersuchungsbereichs. Dieser Name wird in der Tabelle im Fenster **Untersuchungsbereiche** angezeigt.

	Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung dieses Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, verarbeitet die App diesen Untersuchungsbereich während ihrer Ausführung. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die App diesen Untersuchungsbereich während ihrer Ausführung nicht. Sie können diesen Bereich zu einem späteren Zeitpunkt zu den Betriebseinstellungen der Komponente hinzufügen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Diese Einstellungsgruppe ermöglicht die Konfiguration des Untersuchungsbereichs. In der Dropdown-Liste der Dateisysteme können Sie den Typ des Dateisystems auswählen: • **Lokal** (Standardwert) – Lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie den Pfad zu einem lokalen Verzeichnis angeben. • **Mounted** – Gemountete Remote-Verzeichnisse oder lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie das Protokoll oder den Namen des Dateisystems angeben. • **Freigegeben** – Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind. • **Alle freigegebenen** – Alle Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind.
	Wenn in der Drop-down-Liste der Dateisysteme der Typ **Alle** oder **Mounted** ausgewählt ist, können Sie rechts in der Drop-down-Liste das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind.
	Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Untersuchungsbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie Masken und Tags verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

	Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardmäßige Pfadangabe **/** – Die App untersucht alle Verzeichnisse des lokalen Dateisystems. Wenn in der Dropdown-Liste der Dateisysteme als Typ **Lokal** ausgewählt ist und kein Pfad angegeben wird, untersucht die App alle Verzeichnisse des lokalen Dateisystems.
Name des Dateisystems	Eingabefeld für den Namen des Dateisystems, auf dem sich die Verzeichnisse befinden, die Sie zum Untersuchungsbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste auf der rechten Seite das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der App während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster. Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Einstellungen des Untersuchungsbereichs"

In diesem Fenster können Sie die Einstellungen für die Untersuchung während der Ausführung der Aufgabe zur Untersuchung wichtiger Bereiche konfigurieren. Die App ermöglicht die Untersuchung der Dateien, Bootsektoren, der Autostart-Objekte, des Prozess- und des Kernelspeichers.

Einstellungen des Untersuchungsbereichs

Einstellung	Beschreibung
Dateien untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Dateien. Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security Dateien. Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security keine Dateien. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Bootsektoren untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Bootsektoren. Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security Bootsektoren. Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security keine Bootsektoren. Das Kontrollkästchen ist standardmäßig aktiviert.
Kernelspeicher und gestartete Prozesse untersuchen.	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung des Arbeitsspeichers des Geräts. Wenn diese Option aktiviert ist, überprüft Kaspersky Endpoint Security den Kernel-Speicher und die gestarteten Prozesse. Wenn diese Option deaktiviert ist, überprüft Kaspersky Endpoint Security den Kernel-Speicher und die gestarteten Prozesse nicht. Das Kontrollkästchen ist standardmäßig aktiviert.
Autostart-Objekte untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Autostart-Objekten. Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Endpoint Security Autostart-Objekte. Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security keine Autostart-Objekte. Das Kontrollkästchen ist standardmäßig aktiviert.
Zu untersuchende Geräte	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Untersuchungsbereiche** öffnet. In diesem Fenster können Sie die Geräte angeben, deren Bootsektoren untersucht werden sollen.
Globale Ausnahmen verwenden	Das Kontrollkästchen aktiviert oder deaktiviert den Ausschluss von in den globalen Ausnahmen angegeben Mountpunkten während der App-Ausführung. Wenn diese Option aktiviert ist, schließt die App die konfigurierten Mountpunkte von der Untersuchung aus. Das Kontrollkästchen ist standardmäßig aktiviert.
Ausschlüsse aus dem Schutz vor	Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung konfigurierter Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der App-Ausführung.

bedrohlichen Dateien verwenden	Wenn das Kontrollkästchen aktiviert ist, schließt die App jene Objekte von der Untersuchung aus, die in den Ausschlüssen der Komponente "Schutz vor bedrohlichen Dateien" angegeben sind. Das Kontrollkästchen ist standardmäßig aktiviert.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält die Masken der Gerätenamen, deren Bootsektoren die App untersuchen soll. Standardmäßig enthält die Tabelle die Gerätenamen-Maske **/**** (alle Geräte).

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Untersuchungseinstellungen"

In diesem Fenster können Sie die Einstellungen für die Untersuchung von Dateien durch die Aufgabe konfigurieren.

Untersuchungseinstellungen

Einstellung	Beschreibung
Archive untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Archiven. Wenn das Kontrollkästchen aktiviert ist, so untersucht die App Archive. Um ein Archiv zu untersuchen, muss es zunächst von der App entpackt werden, was die Untersuchung verlangsamen kann. Sie können die Dauer der Untersuchung von Archiven reduzieren, indem Sie im Abschnitt **Allgemeine Untersuchungseinstellungen** die Einstellungen **Dateien überspringen, deren Untersuchung länger dauert als (Sek.)** und/oder **Dateien überspringen, die größer sind als (MB)** konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Archive. Das Kontrollkästchen ist standardmäßig aktiviert.
Selbstentpackende Archive untersuchen	Das Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung *selbstentpackender Archive (self-extracting archives)*. Selbstentpackende Archive sind Archive, die ein ausführbares Modul zum Entpacken enthalten. Wenn das Kontrollkästchen aktiviert ist, untersucht die App selbstentpackende Archive.

	Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine selbstentpackenden Dateien. Dieses Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Archive untersuchen** deaktiviert ist. Das Kontrollkästchen ist standardmäßig aktiviert.
Mail-Datenbanken untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Mail-Datenbanken der Anwendungen Microsoft Outlook, Outlook Express, The Bat! und anderen E-Mail-Clients. Wenn das Kontrollkästchen aktiviert ist, untersucht die App die Dateien von Mail-Datenbanken. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Dateien von Mail-Datenbanken. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Dateien in Mail-Formaten untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Dateien von E-Mail-Nachrichten im Textformat (plain text). Wenn das Kontrollkästchen aktiviert ist, untersucht die App E-Mail-Nachrichten im Textformat. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App E-Mail-Nachrichten im Textformat nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Dateien überspringen, deren Untersuchung länger dauert als (Sek.)	In diesem Feld können Sie die erlaubte Höchstdauer für die Untersuchung der Datei in Sekunden angeben. Nach Ablauf des angegebenen Zeitraums bricht die App die Untersuchung der Datei ab. Zulässige Werte: 0–9999. Ist der Wert 0 angegeben, dann ist die Untersuchungsdauer nicht beschränkt. Standardwert: 0.
Dateien überspringen, die größer sind als (MB)	In diesem Feld können Sie die maximale Größe der untersuchten Datei in Megabyte angeben. Zulässige Werte: 0–999999. Ist der Wert 0 angegeben, untersucht die App Dateien jeder Größe. Standardwert: 0.
Virenfreie Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectProcessed*. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Unverarbeitete Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectNotProcessed*, wenn eine Datei während der Untersuchung nicht verarbeitet werden kann. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *ObjectNotProcessed*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *ObjectNotProcessed*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Gepackte Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *PackedObjectDetected* für alle erkannten gepackten Objekte.

	Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *PackedObjectDetected*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *PackedObjectDetected*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
iChecker-Technologie verwenden	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung nur neuer oder seit der letzten Untersuchung geänderter Dateien. Wenn das Kontrollkästchen aktiviert ist, untersucht die App nur neue oder seit der letzten Untersuchung geänderte Dateien. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App Dateien unabhängig von ihrem Erstellungs- oder Änderungsdatum. Das Kontrollkästchen ist standardmäßig aktiviert.
Heuristische Analyse verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die heuristische Analyse bei der Untersuchung von Dateien. Das Kontrollkästchen ist standardmäßig aktiviert.
Stufe der heuristischen Analyse	Wenn das Kontrollkästchen **Heuristische Analyse verwenden** aktiviert ist, können Sie die Ebene der heuristischen Analyse in der Dropdown-Liste festlegen: • **Oberflächlich** – Die am wenigsten detaillierte Untersuchung, minimale Systembelastung. • **Mittel** – Mittlere Untersuchung, ausgeglichene Systembelastung. • **Tief** – Detaillierteste Untersuchung, maximale Systembelastung. • **Empfohlen** (Standardwert) – Optimale Stufe, die von den Kaspersky-Experten empfohlen wird. Sie bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Geräte.

Fenster "Aktion beim Fund einer Bedrohung"

In diesem Fenster können Sie Aktionen auswählen, die von der App Kaspersky Endpoint Security für gefundene infizierte Objekte ausgeführt werden soll.

Aktionen beim Fund einer Bedrohung

Einstellung	Beschreibung
Erste Aktion	In der Dropdown-Liste können Sie die erste Aktion auswählen, die von der App für das gefundene infizierte Objekt ausgeführt werden soll: • Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Informationen zur Gefahrenstufe der in der Datei erkannten Bedrohung und zur Möglichkeit ihrer Desinfektion (Standardwert). • Objekt **überspringen**.

Zweite Aktion	In dieser Dropdown-Liste können Sie die zweite Aktion auswählen, die von der App für ein infiziertes Objekt ausgeführt werden soll, falls die erste Aktion nicht erfolgreich war: • Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Daten zur in der Datei erkannten Gefahrenstufe der Bedrohung und zur Möglichkeit ihrer Desinfektion. • Objekt **überspringen** (Standardwert).

Abschnitt "Ausschlüsse"

Ausschluss von der Untersuchung – Eine Reihe von Bedingungen, die erfüllt sein müssen, damit die App Kaspersky Endpoint Security Objekte nicht auf Viren und andere Schadsoftware überprüft. Objekte können auch anhand von Masken und Bedrohungsnamen von der Untersuchung ausgeschlossen werden.

Einstellungen der Ausschlüsse von der Untersuchung

Einstellungsgruppe	Beschreibung
Ausschlussbereiche	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausschlussbereiche** öffnet. In diesem Fenster können Sie eine Liste mit Bereichen festlegen, die von der Untersuchung ausgeschlossen werden sollen.
Ausschlüsse nach Maske	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster Ausschlüsse nach Maske öffnet. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren.
Ausschlüsse nach Bedrohungsname	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster Ausschlüsse nach Bedrohungsname öffnet. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren.

Fenster "Ausschlussbereiche"

Die Tabelle enthält Bereiche mit Ausschlüsse von der Untersuchung. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der App angewendet wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "<Neuer Ausschlussbereich>"

In diesem Fenster können Sie einen neuen Bereich mit Untersuchungsausschlüssen hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster Ausschlussbereiche angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss des Bereichs von der Untersuchung während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während ihrer Ausführung von der Untersuchung aus. Wenn das Kontrollkästchen deaktiviert ist, schließt die App diesen Bereich während ihrer Ausführung in die Untersuchung ein. Sie können diesen Bereich zu einem späteren Zeitpunkt ausschließen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Diese Einstellungsgruppe erlaubt die Konfiguration des Ausschlussbereichs. In der Dropdown-Liste der Dateisysteme können Sie den Typ des Dateisystems auswählen, auf dem sich die Verzeichnisse befinden, die von der Untersuchung ausgeschlossen werden sollen: • **Lokal** – Lokale Verzeichnisse. • **Mounted** – Eingebundene Verzeichnisse. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind.
	Wenn in der Drop-down-Liste der Dateisysteme der Typ **Mounted** ausgewählt ist, können Sie rechts in der Drop-down-Liste das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind.

- **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind.

Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Ausschlussbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie Masken und Tags verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

	Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Als Pfad ist standardmäßig **/** angegeben: Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus.
Name des Dateisystems	Eingabefeld für den Namen des Dateisystems, auf dem sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste auf der rechten Seite das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Untersuchung ausgeschlossen werden. Die Masken werden nur auf Objekte innerhalb des Verzeichnisses angewendet, das im Eingabefeld des Pfades angegeben ist. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen. Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist. Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Maske"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren. Die App untersucht keine Dateien, deren Namen die angegebenen Masken enthalten. Standardmäßig ist die Liste mit Masken leer.

Sie können Masken hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist.

Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Bedrohungsname"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren. Die App blockiert die angegebenen Bedrohungen nicht. Standardmäßig ist die Liste mit den Namen von Bedrohungen leer.

Sie können Namen von Bedrohungen hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Bedrohung aus den Ausschlüsse.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens ein Bedrohungsname ausgewählt ist.

Ein Klick auf den Namen einer Bedrohung in der Tabelle öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung ändern, die von der Untersuchung ausgenommen wird.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung angeben, die von der Untersuchung ausgenommen wird.

Untersuchung wichtiger Bereiche über die Befehlszeile

Über die Befehlszeile können Sie mithilfe der vordefinierten Aufgabe zur Untersuchung wichtiger Bereiche (*Critical_Areas_Scan*) wichtige Bereiche des Betriebssystems des geschützten Geräts untersuchen.

Sie können diese Aufgabe manuell starten, beenden, anhalten und fortsetzen und den Zeitplan für den Aufgabenstart konfigurieren. Sie können Untersuchungseinstellungen konfigurieren, indem Sie die Einstellungen für diese Aufgabe ändern.

Einstellungen der Aufgabe zur Untersuchung wichtiger Bereiche

Einstellung	Beschreibung	Werte
`ScanFiles`	Aktiviert die Untersuchung von Dateien.	`Yes` – Dateien untersuchen. `No` (Standardwert) – Dateien nicht untersuchen.
`ScanBootSectors`	Aktiviert die Untersuchung der Bootsektoren.	`Yes` (Standardwert) – Bootsektoren untersuchen. `No` – Bootsektoren nicht untersuchen.
`ScanComputerMemory`	Aktiviert die Untersuchung des Prozess- und Kernelspeichers.	`Yes` (Standardwert) – Prozess-Speicher und Kernelspeicher untersuchen. `No` – Prozess-Speicher und Kernelspeiche nicht untersuchen.
`ScanStartupObjects`	Aktiviert die Untersuchung der Autostart-Objekte.	`Yes` (Standardwert) – Autostart-Objekte untersuchen. `No` – Autostart-Objekte nicht untersucher
`ScanArchived`	Aktiviert die Untersuchung von Archiven (einschließlich selbstentpackender sfx-Archive).	`Yes` (Standardwert) – Archive untersuche Wenn der Wert `FirstAction=Recommended` angegeben ist, löscht die App je nach Archivtyp entweder das infizierte Objekt oder das gesamte Archiv, das die Bedrohung enthält `No` – Archive nicht untersuchen.

	Die App untersucht Archive wie .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Die Liste der unterstützten Archivformate hängt von den verwendeten App-Datenbanken ab.	
`ScanSfxArchived`	Aktiviert die Untersuchung von nur selbstentpackenden Archiven (Archiven, zu deren Bestandteilen ein ausführbares Dekompressionsmodul gehört).	`Yes` (Standardwert) – Selbstentpackende Archive untersuchen. `No` – Selbstentpackende Archive nicht untersuchen.
`ScanMailBases`	Aktiviert die Untersuchung von E-Mail-Datenbanken von Microsoft Outlook, Outlook Express, The Bat und anderer Mail-Clients.	`Yes` – Dateien von E-Mail-Datenbanken untersuchen. `No` (Standardwert) – Dateien von E-Mail-Datenbanken nicht untersuchen.
`ScanPlainMail`	Aktiviert die Untersuchung von E-Mail-Nachrichten im Textformat (plain text).	`Yes` – E-Mail-Nachrichten im Textformat untersuchen. `No` (Standardwert) – E-Mail-Nachrichten in Textformat nicht untersuchen.
`SizeLimit`	Maximale Größe des zu untersuchenden Objekts (in Megabyte). Wenn die Größe des zu untersuchenden Objekts den angegebenen Wert überschreitet, überspringt die App das Objekt während der Untersuchung.	0 – 999999 0 – Die App untersucht Objekte beliebiger Größe. Standardwert: 0.
`TimeLimit`	Maximale Untersuchungsdauer (in Sekunden) eines Objekts. Die App stellt die Untersuchung eines Objekts ein, wenn sie länger dauert als durch diese Einstellung festgelegt.	0 – 9999 0 – die Untersuchungsdauer für Objekte ist nicht begrenzt. Standardwert: 0.
`FirstAction`	Auswahl der ersten Aktion, welche die App für infizierte Objekte ausführen soll.	`Disinfect` (desinfizieren) – Die App versucht, ein Objekt zu desinfizieren, und speichert eine Kopie davon im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder der Typ der Bedrohung im Objekt nicht desinfiziert werden kann), belässt die App das Objekt unverändert. Wenn die erste Aktion auf `Desinfizieren` festgelegt ist, wird empfohlen, die zweite Aktion mithilfe der Einstellung `SecondAction` anzugeben `Remove` (löschen) – Die App löscht das infizierte Objekt, nachdem eine Backup-Kopie davon erstellt wurde.

		`Recommended` (empfohlene Aktion ausführen) – Die App wählt automatisch eine Aktion für das Objekt und führt sie au wobei Informationen zu der im Objekt gefundenen Bedrohung berücksichtigt werden. Beispielsweise löscht Kaspersky Endpoint Security Trojaner sofort, da sie andere Dateien nicht infizieren und deshalb keine Desinfektion erfordern. `Skip` (überspringen) – Die App unternimm keinen Versuch, das infizierte Objekt zu desinfizieren oder zu löschen. Informatione über das infizierte Objekt werden im Protokoll gespeichert. Standardwert: `Recommended`
`SecondAction`	Auswahl der zweiten Aktion, welche die App für infizierte Objekte ausführen soll. Die App führt die zweite Aktion aus, wenn die Ausführung der ersten Aktion misslingt.	Die Werte der Einstellung `SecondAction` sind dieselben wie die Werte der Einstellun `FirstAction`. Wenn als erste Aktion `Skip` oder `Remove` ausgewählt ist, muss keine zweite Aktion angegeben werden. In allen anderen Fällen wird empfohlen, zwei Aktionen anzugeben. Wenn Sie keine zweite Aktion angegeben haben, wendet die App `Skip` (überspringe als zweite Aktion an. Standardwert: `Skip`
`UseExcludeMasks`	Aktiviert den Ausschluss von Objekten, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, von der Untersuchung.	`Yes` – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, aus der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht aus der Untersuchur ausschließen.

`ExcludeMasks.item_#`	Ausschluss von der Untersuchung von Objekten nach Name oder Maske. Mit dieser Einstellung können Sie eine einzelne Datei anhand des Namens oder mehrere Dateien anhand von Masken im Shell-Format aus dem angegebenen Untersuchungsbereich ausschließen.
	Bevor Sie den Wert dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseExcludeMasks` aktiviert ist.
		Der Standardwert ist nicht angegeben.
		Beispiel:
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Aktiviert den Ausschluss von Objekten mit Bedrohungen, die durch die Einstellung `ExcludeThreats.item_#` festgelegt sind, von der Untersuchung.	`Yes` – Objekte, die Bedrohungen enthalter die in der Einstellung `ExcludeThreats.item_#` angegeben sin von der Untersuchung ausschließen.

		`No` (Standardwert) – Objekte, die Bedrohungen enthalten, die in der Einstellung `ExcludeThreats.item_#` angegeben sind, nicht von der Untersuchur ausschließen.

`ExcludeThreats.item_#`	Schließt Objekte nach dem Namen der in den Objekten gefundenen Bedrohungen von der Untersuchung aus. Bevor Sie die Werte dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseExcludeThreats` aktiviert ist.
	Um ein Objekt von der Untersuchung auszuschließen, geben Sie den vollständigen Namen der Bedrohung an, die im Objekt gefunden wurde, d. h. die Zeile mit der Entscheidung der App, dass dieses Objekt infiziert ist.
	Sie können beispielsweise ein Tool zum Sammeln von Informationen über Ihr Netzwerk verwenden. Damit es von der App nicht blockiert wird, fügen Sie den vollständigen Namen der darin enthaltenen Bedrohung zur Liste der Bedrohungen hinzu, die von der Untersuchung ausgenommen sind.
	Den vollständigen Namen der im Objekt gefundenen Bedrohung finden Sie im Protokoll der App oder auf der Website https://threats.kaspersky.com.
		Beim Wert der Einstellung muss die Groß- und Kleinschreibung beachtet werden.
		Der Standardwert ist nicht angegeben.
		Beispiel:
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Aktivieren der Verwendung von globalen Ausnahmen während der Untersuchung.	`Yes` (Standardwert) – Globale Ausnahmen verwenden. `No` – Keine globale Ausnahmen verwenden
`UseOASExclusions`	Aktivieren der Verwendung der Ausnahmen des Schutzes vor bedrohlichen Dateien während der Untersuchung.	`Yes` (Standardwert) – Ausnahmen des Schutzes vor bedrohlichen Dateien verwenden. `No` – Keine Ausnahmen des Schutzes vor bedrohlichen Dateien verwenden.
`ReportCleanObjects`	Aktiviert die Protokollierung von Informationen zu untersuchten Objekten, welche die App als nicht infiziert einstuft. Sie können diese Einstellung aktivieren, um beispielsweise sicherzustellen, dass ein bestimmtes Objekt durch die App untersucht wurde.	`Yes` – Informationen zu nicht infizierten Objekten im Protokoll speichern. `No` (Standardwert) – Informationen zu nicht infizierten Objekten nicht im Protokoll speichern.

`ReportPackedObjects`	Aktiviert das Protokollieren von Informationen über untersuchte Objekte, die Bestandteil zusammengesetzter Objekte sind. Sie können diese Einstellung aktivieren, um beispielsweise sicherzustellen, dass ein bestimmtes Objekt innerhalb eines Archivs von der App untersucht wurde.	`Yes` – Informationen über die Untersuchur von Objekten, die zu einem Archiv gehören im Protokoll speichern. `No` (Standardwert) – Informationen über d Untersuchung von Objekten, die zu einem Archiv gehören, nicht im Protokoll speicher
`ReportUnprocessedObjects`	Aktiviert das Protokollieren von Informationen über Objekte, die aus einem bestimmten Grund nicht verarbeitet wurden.	`Yes` – Informationen zu nicht verarbeitete Objekten im Protokoll speichern. `No` (Standardwert) – Informationen zu nich verarbeiteten Objekten nicht im Protokoll speichern.
`UseAnalyzer`	Aktiviert die heuristische Analyse. Mithilfe der heuristischen Analyse kann die App Bedrohungen bereits erkennen, bevor sie den Virenanalysten bekannt sind.	`Yes` (Standardwert) – Heuristische Analys aktivieren. `No` – Heuristische Analyse deaktivieren.
`HeuristicLevel`	Legt die Stufe der heuristischen Analyse fest. Sie können die Ebene der heuristischen Analyse festlegen. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Gründlichkeit der Suche nach Bedrohungen, der Belastung der Betriebssystemressourcen und der Untersuchungsdauer. Je höher die festgelegte Ebene der heuristischen Analyse, desto mehr Ressourcen verbraucht die Untersuchung und desto länger dauert sie.	`Light` – Oberflächlichste Untersuchung m minimaler Belastung des Systems. `Medium` – Mittlere Ebene der heuristischer Analyse mit ausgeglichener Belastung des Betriebssystems. `Deep` – Gründlichste Untersuchung mit maximaler Belastung des Betriebssystems. `Recommended` (Standardwert) – Der empfohlene Wert.
`UseIChecker`	Aktiviert die Nutzung der iChecker-Technologie.	`Yes` (Standardwert) – Nutzung der iChecker-Technologie aktivieren. `No` – Nutzung der iChecker-Technologie deaktivieren.
`DeviceNameMasks.item_#`	Liste mit Namen der Geräte, deren Bootsektoren von der App untersucht werden. Der Einstellungswert darf nicht leer sein. Um die Aufgabe auszuführen, müssen Sie mindestens eine Maske für Gerätenamen angeben.	`AllObjects` – Untersuchung der Bootsektoren aller Geräte. `<Maske für Gerätenamen>` – Untersuchung der Bootsektoren von den Geräten, deren Namen von der Maske eingeschlossen werden. Standardwert: `/**` (beliebiger Zeichensatz im Gerätenamen, einschließlich des Zeiche `/`)

Der Abschnitt **[ScanScope.item_#]** enthält die folgenden Parameter:

`AreaDesc`	Beschreibung des Untersuchungsbereichs mit zusätzlichen Informationen über den Untersuchungsbereich. Die maximale Länge einer Zeichenfolge, die mit dieser Einstellung angegeben werden kann, beträgt 4096 Zeichen.	Standardwert: `All objects`. Beispiel: `AreaDesc="Mail bases scan"`
`UseScanArea`	Aktiviert die Untersuchung des angegebenen Bereichs. Um die Aufgabe auszuführen, müssen Sie mindestens einen zu untersuchenden Bereich angeben.	`Yes` (Standardwert) – Den angegebenen Bereich untersuchen. `No` – Angegebenen Bereich nicht untersuchen.
`AreaMask.item_#`	Einschränkung des Untersuchungsbereichs. Im Untersuchungsbereich untersucht die App nur Dateien, die mit Masken im Shell-Format angegeben wurden. Wenn die Einstellung nicht angegeben wurde, untersucht die App alle Objekte im Untersuchungsbereich. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: * (alle Objekte untersucher Beispiel: `AreaMask.item_<Nummer des Elements>=*doc`
`Path`	Pfad zum Verzeichnis mit untersuchten Objekten.	`<Pfad zum lokalen Verzeichnis>` – Objekte im angegebenen Verzeichnis untersuchen. `Shared:NFS` – Ressourcen des Gerätedateisystems untersuchen, auf die über das NFS-Protokoll zugegriffen wird. `Shared:SMB` – Ressourcen des Gerätedateisystems untersuchen, auf die über das Samba-Protokoll zugegriffen wird `Mounted:NFS` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über NFS-Protokoll eingebunden sind. `Mounted:SMB` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über das Samba-Protokoll eingebunden sind. `AllRemoteMounted` – alle Remote-Verzeichnisse untersuchen, die auf dem Gerät über Samba- oder NFS-Protokolle gemountet sind. `AllShared` – Ressourcen des Gerätedateisystems untersuchen, auf die über das Samba- und NFS-Protokoll zugegriffen wird. `<Typ des Dateisystems>` – alle Ressourcen des angegebenen Dateisysten des Geräts untersuchen.

Der Abschnitt **[ExcludedFromScanScope.item_#]** enthält die folgenden Parameter:

`AreaDesc`	Beschreibung des Ausschlussbereichs von der Untersuchung mit zusätzlichen Informationen über den Ausschlussbereich.	Der Standardwert ist nicht angegeben.
`UseScanArea`	Schließt den angegebenen Bereich von der Untersuchung aus.	`Yes` (Standardwert) – Den angegebenen Bereich ausschließen. `No` – Den angegebenen Bereich nicht ausschließen.
`AreaMask.item_#`	Einschränkung des von der Untersuchung ausgeschlossenen Bereichs. Im Ausschlussbereich schließt die App nur Dateien aus, die mittels Masken im Shell-Format angegeben wurden. Wenn die Einstellung nicht angegeben wurde, schließt die App alle Objekte im Ausschlussbereich aus. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: `*` (alle Objekte ausschließer
`Path`	Pfad zum Verzeichnis mit ausgeschlossenen Objekten.	`<Pfad zum lokalen Verzeichnis>` – Objekte im angegebenen Verzeichnis von der Untersuchung ausschließen. Bei der Angabe des Pfades können Sie Masken verwenden.

Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Bei Systemen mit dem Dateisystem BTRFS und aktivierten aktiven Snapshots wird es zur Optimierung der Untersuchungsaufgaben empfohlen, den Pfad mit dem im "Read only"-Modus gemounteten Snapshots den Ausschlüsse hinzuzufügen. Beispielsweise können in Systemen auf Basis von SUSE/OpenSUSE eines Ausschluss folgendermaßen angeben `/.snapshots/*/snapshot/`.

`<Pfad zum lokalen Verzeichnis>` – Objekte im angegebenen Verzeichnis (und dessen Unterverzeichnissen) von der Untersuchung ausschließen. Bei der Angab des Pfades können Sie Masken verwenden

Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Bei Systemen mit dem Dateisystem BTRFS und aktivierten aktiven Snapshots wird es zur Optimierung der Untersuchungsaufgaben empfohlen, den Pfad mit dem im "Read only"-Modus gemounteten Snapshots den Ausschlüsse hinzuzufügen. Beispielsweise können in Systemen auf Basis von SUSE/OpenSUSE eines Ausschluss folgendermaßen angeben `/.snapshots/*/snapshot/`.

`Mounted:NFS` – Remote-Verzeichnisse, di auf dem Gerät über das NFS-Protokoll gemountet sind, von der Untersuchung ausschließen.

`Mounted:SMB` – Remote-Verzeichnisse, di auf dem Gerät über das Samba-Protokoll gemountet sind, von der Untersuchung ausschließen.

`AllRemoteMounted` – Alle Remote-Verzeichnisse, die auf dem Gerät über Samba- oder NFS-Protokolle gemountet sind, von der Untersuchung ausschließen.

`< Typ des Dateisystems >` – alle Ressourcen des angegebenen Dateisysten des Geräts von der Untersuchung ausschließen.

		Remote-Verzeichnisse werden nur dann von der Untersuchung durch die App ausgeschlossen, wenn sie bereits vor dem Aufgabenstart eingebunden wurden. Remote-Verzeichnisse, die erst nach dem Aufgabenstart eingebunden wurden, werden von der Untersuchung nicht ausgeschlossen.

Untersuchung von Wechseldatenträgern

Kaspersky Endpoint Security kann die folgenden Wechseldatenträger bei Anschluss an das geschützte Gerät untersuchen: CD-/DVD-Laufwerke, Blu-ray-Discs, Flash-Laufwerke (einschließlich USB-Modems), externe Festplatten und Disketten.

Wenn die Untersuchung von Wechseldatenträgern aktiviert ist, überwacht Kaspersky Endpoint Security die Verbindung von Wechseldatenträgern mit dem geschützten Gerät und untersucht, wenn ein angeschlossener Wechseldatenträger erkannt wird, das Laufwerk und seine Bootsektoren auf Viren und andere Malware.

Standardmäßig kontrolliert die App den Anschluss von Wechseldatenträgern nicht und untersucht sie auch nicht.

Diese Funktionalität wird im KESL-Container nicht unterstützt.

Untersuchung von Wechseldatenträgern in der Web Console konfigurieren

In der Web Console können Sie Einstellungen zur Untersuchung von Wechseldatenträgern in den Einstellungen der Richtlinie konfigurieren (**App-Einstellungen** → **Lokale Aufgaben** → **Untersuchung von Wechseldatenträgern**).

Einstellungen der Komponente "Untersuchung von Wechseldatenträgern"

Einstellung	Beschreibung
Untersuchung von Wechseldatenträgern aktiviert/deaktiviert	Der Umschalter aktiviert und deaktiviert die Untersuchung von Wechseldatenträgern bei ihrem Anschluss an das Gerät. Der Schalter ist standardmäßig deaktiviert.
Aktion beim Anschließen eines Wechseldatenträgers	In der Dropdown-Liste können Sie die Aktion auswählen, die von der App beim Verbinden von Wechseldatenträgern mit dem Benutzergerät ausgeführt werden: • Wechseldatenträger beim Verbinden **nicht untersuchen** (Standardwert). • **Schnelle Untersuchung** – Es werden nur Dateien bestimmter Typen auf Wechseldatenträgern (außer CD-/DVD-Laufwerken und Blu-ray-Discs) untersucht und es werden keine zusammengesetzten Objekte entpackt. Die schnelle Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Untersuchung wichtiger Bereiche* durchgeführt. Auf Wechseldatenträgern werden die folgenden Dateiformate überprüft: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • **Gründliche Untersuchung** – Dient zur Untersuchung aller Dateien auf Wechseldatenträgern (außer CD/DVD-Laufwerken und Blu-ray-Discs). Die genaue Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Schadsoftware-Untersuchung* durchgeführt.
Aktion beim Anschließen eines CD-/DVD-Laufwerks	In dieser Dropdown-Liste können Sie eine Aktion auswählen, die von der App beim Anschluss eines CD-/DVD-Laufwerks oder einer Blu-ray-Disc an das Benutzergerät ausgeführt werden soll:

	• CD-/DVD-Laufwerke und Blu-ray-Discs beim Verbinden **nicht untersuchen** (Standardwert). • **Schnelle Untersuchung** – Untersucht nur Dateien bestimmter Typen auf CD-/DVD-Laufwerken und Blu-ray-Discs. Die schnelle Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Untersuchung wichtiger Bereiche* durchgeführt. Auf Wechseldatenträgern werden die folgenden Dateiformate überprüft: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • **Gründliche Untersuchung** – Untersucht alle Dateien auf CD/DVD-Laufwerken und Blu-ray-Discs. Die genaue Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Schadsoftware-Untersuchung* durchgeführt.
Zugriff auf den Wechseldatenträger während der Untersuchung blockieren	Dieses Kontrollkästchen aktiviert oder deaktiviert das Blockieren von Dateien auf dem angeschlossenen Wechseldatenträger während der Untersuchung. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Untersuchung von Wechseldatenträgern in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie Einstellungen zur Untersuchung von Wechseldatenträgern in den Einstellungen der Richtlinie konfigurieren (**Lokale Aufgaben** → **Untersuchung von Wechseldatenträgern**).

Einstellungen der Komponente "Untersuchung von Wechseldatenträgern"

Einstellung	Beschreibung
Aktiviert die Untersuchung von Wechseldatenträgern bei ihrem Anschluss an das Gerät.	Das Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Wechseldatenträgern bei ihrem Anschluss an das Benutzergerät. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Aktion beim Anschließen eines Wechseldatenträgers	In der Dropdown-Liste können Sie die Aktion auswählen, die von der App beim Verbinden von Wechseldatenträgern mit dem Benutzergerät ausgeführt werden: • Wechseldatenträger beim Verbinden **nicht untersuchen** (Standardwert). • **Schnelle Untersuchung** – Es werden nur Dateien bestimmter Typen auf Wechseldatenträgern (außer CD-/DVD-Laufwerken und Blu-ray-Discs) untersucht und es werden keine zusammengesetzten Objekte entpackt. Die schnelle Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Untersuchung wichtiger Bereiche* durchgeführt.

	Auf Wechseldatenträgern werden die folgenden Dateiformate überprüft: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • **Gründliche Untersuchung** – Dient zur Untersuchung aller Dateien auf Wechseldatenträgern (außer CD/DVD-Laufwerken und Blu-ray-Discs). Die genaue Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Schadsoftware-Untersuchung* durchgeführt.
Aktion beim Anschließen eines CD-/DVD-Laufwerks	In dieser Dropdown-Liste können Sie eine Aktion auswählen, die von der App beim Anschluss eines CD-/DVD-Laufwerks oder einer Blu-ray-Disc an das Benutzergerät ausgeführt werden soll: • CD-/DVD-Laufwerke und Blu-ray-Discs beim Verbinden **nicht untersuchen** (Standardwert). • **Schnelle Untersuchung** – Untersucht nur Dateien bestimmter Typen auf CD-/DVD-Laufwerken und Blu-ray-Discs. Die schnelle Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Untersuchung wichtiger Bereiche* durchgeführt. Auf Wechseldatenträgern werden die folgenden Dateiformate überprüft: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • **Gründliche Untersuchung** – Untersucht alle Dateien auf CD/DVD-Laufwerken und Blu-ray-Discs. Die genaue Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Schadsoftware-Untersuchung* durchgeführt.
Zugriff auf den Wechseldatenträger während der Untersuchung blockieren	Dieses Kontrollkästchen aktiviert oder deaktiviert das Blockieren von Dateien auf dem angeschlossenen Wechseldatenträger während der Untersuchung. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Untersuchung von Wechseldatenträgern über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Untersuchung von Wechseldatenträgern mithilfe der vordefinierten Aufgabe "Untersuchung von Wechseldatenträgern" (*Removable_Drives_Scan*) verwalten.

Die Aufgabe zur Untersuchung von Wechseldatenträgern ist standardmäßig inaktiv. Sie können diese Aufgabe manuell starten und beenden. Sie können Untersuchungseinstellungen konfigurieren, indem Sie die Einstellungen für diese Aufgabe ändern.

Wenn die Aufgabe gestartet wurde, überwacht die App die Verbindung von Wechseldatenträgern mit dem Gerät und erstellt und führt bei Anschluss des Wechseldatenträgers eine temporäre Aufgabe zur Untersuchung von Bootsektoren (Aufgabe vom Typ *ODS*) aus. Diese Aufgabe kann nicht beendet werden. Nach Abschluss der Aufgabe löscht wird sie von der App automatisch gelöscht.

Wenn Sie in den Einstellungen der Aufgabe zur Untersuchung von Wechseldatenträgern die Dateiuntersuchung aktiviert haben, startet die App auch eine oder mehrere temporäre Aufgaben zur benutzerdefinierten Untersuchung von Dateien (Aufgaben vom Typ *ODS*). Bei Bedarf kann ein Benutzer mit Administratorrechten die Ausführung dieser Aufgaben beenden.

Wenn Sie die Einstellungen der Aufgabe zur Untersuchung von Wechseldatenträgern ändern, werden die neuen Werte nicht in bereits laufende temporäre Aufgaben übernommen. Wenn Sie die Aufgabe zur Untersuchung von Wechseldatenträgern beenden, werden bereits laufende temporäre Aufgaben nicht beendet.

Einstellungen der Aufgabe zur Untersuchung von Wechseldatenträgern

Einstellung	Beschreibung	Werte
`ScanRemovableDrives`	Aktiviert die Untersuchung von Wechseldatenträgern sobald diese an das Gerät angeschlossen werden. Diese Einstellung gilt nicht für CD-/DVD-Laufwerke und Blu-ray-Discs (siehe Einstellung `ScanOpticalDrives`).	`DetailedScan` – Alle Dateien auf Wechseldatenträgern (außer CD-/DVD-Laufwerken und Blu-ray-Discs) untersuchen. Die detaillierte Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Scan_File* (ID:3) durchgeführt. `QuickScan` – Es werden nur Dateien bestimmter Typen auf Wechseldatenträgern (außer CD-/DVD-Laufwerken und Blu-ray-Discs) untersucht. Auf Wechseldatenträgern werden die folgenden Dateiformate überprüft: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. Die schnelle Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Critical_Areas_Scan* (ID:4) durchgeführt. `NoScan` (Standardwert) – Keine Wechseldatenträger bei ihrem Anschluss untersuchen.
`ScanOpticalDrives`	Aktiviert die Untersuchung von CD-/DVD-Laufwerken und Blu-ray-Discs, sobald diese an das Gerät angeschlossen werden.	`DetailedScan` – Alle Dateien auf CD-/DVD-Laufwerken und Blu-ray-Discs untersuchen. Die detaillierte Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Scan_File* (ID:3) durchgeführt. `QuickScan` – Untersucht nur Dateien bestimmter Typen auf CD-/DVD-Laufwerken und Blu-ray-Discs.

		Auf Wechseldatenträgern werden die folgenden Dateiformate überprüft: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. Die schnelle Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Critical_Areas_Scan* (ID:4) durchgeführt. `NoScan` (Standardwert) – Beim Anschluss von CD-/DVD-Laufwerken und Blu-ray-Discs keine Untersuchung ausführen
`BlockDuringScan`	Aktivierung der Blockierung von Dateien auf dem angeschlossenen Datenträger während der Untersuchung. Während der Untersuchung von Bootsektoren werden Dateien nicht blockiert.	`Yes` – Dateien während der Untersuchung blockieren. `No` (Standardwert) – Dateien während der Untersuchung nicht blockieren.

Untersuchung von Containern

Sie können die Untersuchung von Containern und Images auf Schadsoftware in Echtzeit und auf Befehl durchführen:

- Mit der Komponente *Container-Überwachung* können Sie gestartete Container und Namespaces in Echtzeit untersuchen.
- Mithilfe von Aufgaben vom Typ *Untersuchung von Containern* können Sie Container und Images auf Befehl untersuchen.

Die App unterstützt die Integration mit dem System zur Verwaltung von Docker-Containern, der CRI-O-Umgebung und den Tools Podman und runc.

Um die Aufgaben zur Untersuchung von Containern nutzen zu können, benötigen Sie eine Lizenz, in der diese Funktion enthalten ist.

Container-Überwachung

Standardmäßig ist die Komponente "Container-Überwachung" aktiviert. Die App untersucht gestartete Container und Namespaces in Echtzeit.

Damit die Komponente "Container-Überwachung" funktioniert, muss die Komponente Schutz vor bedrohlichen Dateien aktiviert sein. Bei der Untersuchung von Containern und Namespaces werden Einstellungen zum Schutz vor bedrohlichen Dateien verwendet.

Die App prüft keine Namespaces und Container, es sei denn, auf dem Betriebssystem sind Komponenten für die Arbeit mit Containern und Namespaces installiert. In diesem Fall wird der Status der Komponente "Container-Überwachung" in der Befehlszeile als `Aufgabe ist verfügbar und wird nicht ausgeführt` angezeigt und in Kaspersky Security Center als `Beendet`.

Sie können die Komponente „Container-Überwachung“ aktivieren oder deaktivieren sowie die Einstellungen der Container-Untersuchung und Namespaces in Echtzeit konfigurieren:

- Sie können eine Aktion auswählen, die von der App beim Fund eines infizierten Objekts für den Container ausgeführt werden soll.

  Dieser Parameter ist verfügbar, wenn die App im Rahmen einer Lizenz verwendet wird, von der diese Funktion abgedeckt wird.

- Sie können die Integration von Kaspersky Endpoint Security mit dem System zur Verwaltung von Docker-Containern, der CRI-O-Umgebung und den Tools Podman und runc konfigurieren.

Container-Überwachung in der Web Console konfigurieren

In der Web Console können Sie die Ausführung der Komponente *Containern-Überwachung* in den Einstellungen der Richtlinie verwalten (**App-Einstellungen → Allgemeine Einstellungen → Einstellungen der Untersuchung von Containern**).

Einstellungen der Container-Überwachung

Einstellung	Beschreibung
Die Untersuchung von Namespaces und Containern ist aktiviert oder deaktiviert.	Dieser Schalter aktiviert oder deaktiviert die Untersuchung von Namespaces und Containern in Echtzeit. Der Schalter ist standardmäßig aktiviert.
Aktion mit Container beim Fund einer Bedrohung	Sie können eine Aktion auswählen, die von der App beim Fund eines infizierten Objekts für den Container ausgeführt werden soll: • **Container überspringen** – Wenn ein infiziertes Objekt erkannt wird, führt die App keine Aktion für den Container aus. • **Container anhalten** – Wenn ein infiziertes Objekt erkannt wird, hält die App den Container an. • **Container anhalten, falls Desinfektion fehlschlägt** (Standardwert) – Wenn die Desinfektion eines infizierten Objekts fehlgeschlagen ist, hält die App den Container an. Dieser Parameter ist verfügbar, wenn die App im Rahmen einer Lizenz verwendet wird, die diese Funktion einschließt.
Docker verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Verwendung der Docker-Umgebung. Das Kontrollkästchen ist standardmäßig aktiviert.
Pfad zum Docker-Socket	Eingabefeld für Pfad oder URI (Uniform Resource Identifier) des Docker-Sockets. Der Standardwert ist /var/run/docker.sock.
CRI-O verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Verwendung der CRI-O-Umgebung. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateipfad	Eingabefeld für den Pfad zur CRI-O-Konfigurationsdatei. Standardwert: /etc/crio/crio.conf.
Podman verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Verwendung des Podman-Tools. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateipfad	Eingabefeld für den Pfad zur ausführbaren Datei des Podman-Tools. Der Standardwert ist /usr/bin/podman.
Stammverzeichnis	Eingabefeld für den Pfad zum Stammverzeichnis des Container-Speichers. Der Standardwert ist /var/lib/containers/storage.
Runc verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Verwendung des runc-Tools. Das Kontrollkästchen ist standardmäßig aktiviert.

Dateipfad	Eingabefeld für den Pfad zur ausführbaren Datei des runc-Tools. Der Standardwert ist: /usr/bin/runc.
Stammverzeichnis	Eingabefeld für den Pfad zum Stammverzeichnis des Speichers für den Container-Status. Der Standardwert ist /run/runc.

Container-Überwachung in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Ausführung der Komponente "Containern-Überwachung" in den Einstellungen der Richtlinie verwalten (**Allgemeine Einstellungen** → **Einstellungen der Untersuchung von Containern**).

Einstellungen der Container-Überwachung

Einstellung	Beschreibung
Untersuchung von Namespaces und Containern aktivieren	Dieses Kontrollkästchen aktiviert oder deaktiviert die Untersuchung von Namespaces und Containern in Echtzeit. Das Kontrollkästchen ist standardmäßig aktiviert.
Aktion mit Container beim Fund einer Bedrohung	In dieser Dropdown-Liste können Sie eine Aktion auswählen, die von der App beim Fund eines infizierten Objekts für den Container ausgeführt werden soll: • **Container überspringen** – Wenn ein infiziertes Objekt erkannt wird, führt die App keine Aktion für den Container aus. • **Container anhalten** – Wenn ein infiziertes Objekt erkannt wird, hält die App den Container an. • **Anhalten, falls Desinfektion fehlschlägt** (Standardwert) – Wenn die Desinfektion eines infizierten Objekts fehlgeschlagen ist, hält die App den Container an. Dieser Parameter ist verfügbar, wenn die App im Rahmen einer Lizenz verwendet wird, die diese Funktion einschließt.
Einstellungen der Untersuchung von Containern	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Einstellungen der Untersuchung von Containern** öffnet.

Fenster "Einstellungen der Container-Untersuchung"

In diesem Fenster können Sie die Integrationseinstellungen von Kaspersky Endpoint Security mit dem Docker-System zur Containerverwaltung, der CRI-O-Umgebung und den Tools Podman und runc konfigurieren.

Einstellungen der Untersuchung von Containern

Einstellung	Beschreibung
Docker verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Verwendung der Docker-Umgebung. Das Kontrollkästchen ist standardmäßig aktiviert.

Pfad zum Docker-Socket	Eingabefeld für Pfad oder URI (Uniform Resource Identifier) des Docker-Sockets. Der Standardwert ist /var/run/docker.sock.
CRI-O verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Verwendung der CRI-O-Umgebung. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateipfad	Eingabefeld für den Pfad zur CRI-O-Konfigurationsdatei. Standardwert: /etc/crio/crio.conf.
Podman verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Verwendung des Podman-Tools. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateipfad	Eingabefeld für den Pfad zur ausführbaren Datei des Podman-Tools. Der Standardwert ist /usr/bin/podman.
Stammverzeichnis	Eingabefeld für den Pfad zum Stammverzeichnis des Container-Speichers.
Runc verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Verwendung des runc-Tools. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateipfad	Eingabefeld für den Pfad zur ausführbaren Datei des runc-Tools. Der Standardwert ist /usr/bin/runc.
Stammverzeichnis	Eingabefeld für den Pfad zum Stammverzeichnis des Speichers für den Container-Status. Der Standardwert ist /run/runc.

Container-Überwachung über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Echtzeitüberwachung von Namespaces und Containern mit der Option `NamespaceMonitoring=Yes/No` in den Allgemeinen App-Einstellungen aktivieren oder deaktivieren.

Sie können den Wert der Einstellung `NamespaceMonitoring` mithilfe der Konfigurationsdatei, die alle allgemeinen App-Einstellungen enthält, oder mithilfe von Befehlszeilenschaltern ändern.

Für die Echtzeituntersuchung von Namespaces und Containern werden die allgemeinen Einstellungen der Container-Untersuchung verwendet. Sie können diese Einstellungen mithilfe spezieller Verwaltungsbefehle für Kaspersky Endpoint Security anzeigen und ändern:

- Sie können die aktuellen Werte der allgemeinen Einstellungen für die Container-Untersuchung in die Konsole oder in eine Konfigurationsdatei ausgeben. Mit dieser Datei können Sie Einstellungen ändern.
- Sie können alle allgemeinen Einstellungen der Container-Untersuchung mithilfe der Konfigurationsdatei ändern, die die Einstellungen enthält. Sie können die Konfigurationsdatei mit dem Befehl zur Ausgabe der allgemeinen Einstellungen für die Container-Untersuchung abrufen.
- Sie können einzelne Einstellungen mithilfe von Befehlszeilenschaltern im Format `< Name der Einstellung >= < Wert der Einstellung >` ändern. Mit dem Befehl zur Ausgabe der allgemeinen Einstellungen für die Container-Untersuchung können Sie die aktuellen Werte der Einstellungen abrufen.

Um die aktuellen Werte der allgemeinen Einstellungen für die Container-Untersuchung in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-container-settings [--json]
```

Wobei gilt: `--json` – Gibt Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Um die aktuellen Werte der allgemeinen Einstellungen für die Container-Untersuchung in eine Datei auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-container-settings --file <Pfad der Konfigurationsdatei> [--json]
```

Wobei gilt:

- `--file <Pfad der Konfigurationsdatei>` – Pfad der Konfigurationsdatei, in der die allgemeinen Einstellungen der Container-Untersuchung gespeichert werden. Wenn Sie den Dateinamen eingeben, ohne einen Dateipfad vorzugeben, wird die Datei im aktuellen Verzeichnis erstellt. Ist unter dem gewünschten Pfad bereits eine Datei mit gleichem Namen vorhanden, wird diese überschreiben. Falls das von Ihnen vorgegebene Verzeichnis auf der Festplatte nicht existiert, wird die Datei nicht erstellt.
- `--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

So ändern Sie die Werte der allgemeinen Einstellungen für die Container-Untersuchung mithilfe einer Konfigurationsdatei:

1. Geben Sie die allgemeinen Einstellungen der Container-Untersuchung wie oben beschrieben in eine Konfigurationsdatei aus.
2. Ändern Sie die Werte der erforderlichen Einstellungen in der Datei und speichern Sie die Änderungen.
3. Führen Sie den Befehl aus:

   ```
   kesl-control --set-container-settings --file <Pfad der Konfigurationsdatei> [--json]
   ```

   Wobei gilt:

   - `--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei mit den allgemeinen Einstellungen für die Container-Untersuchung.
   - `--json` – Geben Sie diesen Schalter an, wenn Sie Einstellungen aus einer Konfigurationsdatei im JSON-Format importieren. Wenn Sie den Schalter `--json` nicht angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

   Alle in der Datei angegebenen Werte der allgemeinen Einstellungen für die Container-Untersuchung werden in die App importiert.

Um die Werte der allgemeinen Einstellungen für die Container-Untersuchung mithilfe von Befehlszeilenschaltern zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-container-settings <Name der Einstellung>=<Wert der Einstellung>
[<Name der Einstellung>=<Wert der Einstellung>]
```

Wobei gilt: `<Name der Einstellung>=<Wert der Einstellung>` – Name und Wert einer der allgemeinen Einstellungen für die Container-Untersuchung.

Die Werte der angegebenen allgemeinen Einstellungen für die Container-Untersuchung werden geändert.

Untersuchung von Containern und Images auf Befehl

Während die Aufgabe zur *Untersuchung von Containern* ausgeführt wird, untersucht Kaspersky Endpoint Security Container und Images auf Viren und andere Malware. Die App kann mehrere Aufgaben zur Untersuchung von Containern gleichzeitig ausführen.

Die Integration des Systems zur Verwaltung von Docker-Containern, der CRI-O-Umgebung und den Tools Podman und runc wird unterstützt.

Um die Aufgabe nutzen zu können, benötigen Sie eine Lizenz, in der diese Funktionalität enthalten ist.

So können Sie die Untersuchung von Containern starten und Untersuchungseinstellungen konfigurieren:

- Geben Sie die zu untersuchenden Container und Bilder nach Name oder Namensmaske an.
- Starten Sie die Untersuchung aller Ebenen von Images und Containern.
- Wählen Sie die Aktion aus, die die App für den Container ausführen soll, und die Aktion, welche die App für das Image ausführen soll, wenn ein infiziertes Objekt erkannt wird.
- Konfigurieren Sie die Einstellungen zur Untersuchung von Objekten in Containern oder Images:
  - Aktivieren und deaktivieren Sie die Untersuchung von Archiven, E-Mail-Datenbanken und E-Mail-Nachrichten im Textformat.
  - Begrenzen Sie die Größe des untersuchten Objekts und die Untersuchungsdauer für das Objekt.
  - Wählen Sie die Aktionen aus, welche die App für infizierte Objekte ausführen soll.
  - Konfigurieren Sie den Ausschluss von Objekten von der Untersuchung nach:
    - Namen oder Masken
    - nach dem Namen der in den Objekten gefundenen Bedrohungen.
  - Aktivieren oder deaktivieren der Verwendung globaler Ausnahmen bei der Untersuchung.
  - Konfigurieren Sie die Verwendung der heuristischen Analyse und der iChecker-Technologie während der Untersuchung.
  - Aktivieren und deaktivieren Sie die Protokollierung von Informationen zu untersuchten nicht infizierten Objekten, zu untersuchten Objekten in Archiven und zu nicht verarbeiteten Objekten.

Untersuchung von Containern in der Web Console

In der Web Console können Sie Container und Images mithilfe der Aufgabe *Untersuchung von Containern* untersuchen.

Sie können Benutzeraufgaben für die Container-Untersuchung erstellen und starten. Sie können die Untersuchungseinstellungen konfigurieren, indem Sie die Aufgabeneinstellungen ändern.

Einstellung	Beschreibung
Archive untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Archiven. Wenn das Kontrollkästchen aktiviert ist, so untersucht die App Archive. Um ein Archiv zu untersuchen, muss es zunächst von der App entpackt werden, was die Untersuchung verlangsamen kann. Sie können die Dauer der Untersuchung von Archiven reduzieren, indem Sie im Abschnitt **Allgemeine Untersuchungseinstellungen** die Einstellungen **Dateien überspringen, deren Untersuchung länger dauert als (Sek.)** und/oder **Dateien überspringen, die größer sind als (MB)** konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Archive. Das Kontrollkästchen ist standardmäßig aktiviert.
Selbstentpackende Archive untersuchen	Das Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung *selbstentpackender Archive (self-extracting archives)*. Selbstentpackende Archive sind Archive, die ein ausführbares Modul zum Entpacken enthalten. Wenn das Kontrollkästchen aktiviert ist, untersucht die App selbstentpackende Archive. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine selbstentpackenden Dateien. Dieses Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Archive untersuchen** deaktiviert ist. Das Kontrollkästchen ist standardmäßig aktiviert.
Mail-Datenbanken untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Mail-Datenbanken der Anwendungen Microsoft Outlook, Outlook Express, The Bat! und anderen E-Mail-Clients. Wenn das Kontrollkästchen aktiviert ist, untersucht die App die Dateien von Mail-Datenbanken. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Dateien von Mail-Datenbanken. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Dateien in Mail-Formaten untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Dateien von E-Mail-Nachrichten im Textformat (plain text). Wenn das Kontrollkästchen aktiviert ist, untersucht die App E-Mail-Nachrichten im Textformat. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App E-Mail-Nachrichten im Textformat nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Dateien überspringen, deren Untersuchung länger dauert als (Sek.)	In diesem Feld können Sie die erlaubte Höchstdauer für die Untersuchung der Datei in Sekunden angeben. Nach Ablauf des angegebenen Zeitraums bricht die App die Untersuchung der Datei ab. Zulässige Werte: 0–9999. Ist der Wert 0 angegeben, dann ist die Untersuchungsdauer nicht beschränkt. Standardwert: 0.
Dateien überspringen, die größer sind als (MB)	In diesem Feld können Sie die maximale Größe der untersuchten Datei in Megabyte angeben. Zulässige Werte: 0–999999. Ist der Wert 0 angegeben, untersucht die App Dateien jeder Größe. Standardwert: 0.

Virenfreie Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectProcessed*. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Unverarbeitete Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectNotProcessed*, wenn eine Datei während der Untersuchung nicht verarbeitet werden kann. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *ObjectNotProcessed*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *ObjectNotProcessed*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Gepackte Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *PackedObjectDetected* für alle erkannten gepackten Objekte. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *PackedObjectDetected*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *PackedObjectDetected*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
iChecker-Technologie verwenden	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung nur neuer oder seit der letzten Untersuchung geänderter Dateien. Wenn das Kontrollkästchen aktiviert ist, untersucht die App nur neue oder seit der letzten Untersuchung geänderte Dateien. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App Dateien unabhängig von ihrem Erstellungs- oder Änderungsdatum. Das Kontrollkästchen ist standardmäßig aktiviert.
Heuristische Analyse verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die heuristische Analyse bei der Untersuchung von Dateien. Das Kontrollkästchen ist standardmäßig aktiviert.
Stufe der heuristischen Analyse	Wenn das Kontrollkästchen **Heuristische Analyse verwenden** aktiviert ist, können Sie die Ebene der heuristischen Analyse in der Dropdown-Liste festlegen: • **Oberflächlich** – Die am wenigsten detaillierte Untersuchung, minimale Systembelastung. • **Mittel** – Mittlere Untersuchung, ausgeglichene Systembelastung. • **Tief** – Detaillierteste Untersuchung, maximale Systembelastung. • **Empfohlen** (Standardwert) – Optimale Stufe, die von den Kaspersky-Experten empfohlen wird. Sie bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Geräte.
Erste Aktion	In der Dropdown-Liste können Sie die erste Aktion auswählen, die von der App für das gefundene infizierte Objekt ausgeführt werden soll: • Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt.

	• Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Informationen zur Gefahrenstufe der in der Datei erkannten Bedrohung und zur Möglichkeit ihrer Desinfektion (Standardwert). • Objekt **überspringen**.
Zweite Aktion	In dieser Dropdown-Liste können Sie die zweite Aktion auswählen, die von der App für ein infiziertes Objekt ausgeführt werden soll, falls die erste Aktion nicht erfolgreich war: • Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Daten zur in der Datei erkannten Gefahrenstufe der Bedrohung und zur Möglichkeit ihrer Desinfektion. • Objekt **überspringen** (Standardwert).
Container untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Containern. Wenn das Kontrollkästchen aktiviert ist, können Sie einen Namen oder eine Namensmaske für Container angeben, die untersucht werden sollen. Das Kontrollkästchen ist standardmäßig aktiviert.
Namensmaske	Eingabefeld für den Namen oder die Maske, welche die zu untersuchenden Container definiert. Standardmäßig ist die Maske * angegeben (alle Container werden untersucht).
Aktion beim Erkennen einer Bedrohung	Sie können eine Aktion auswählen, die von der App beim Fund eines infizierten Objekts für den Container ausgeführt werden soll: • **Container überspringen** – Keine Aktion für den Container ausführen, wenn ein infiziertes Objekt erkannt wird. • **Container anhalten** – Hält den Container an, wenn ein infiziertes Objekt erkannt wird. • **Anhalten, falls Desinfektion fehlschlägt** (Standardwert) – Hält den Container an, wenn die Desinfektion eines infizierten Objekts fehlgeschlagen ist oder die Bedrohung nicht beseitigt werden konnte. Aufgrund von Besonderheiten der Funktionsweise von CRI-O-Umgebungen werden infizierte Objekte in den Containern einer CRI-O-Umgebung weder desinfiziert noch gelöscht. Es wird daher empfohlen, stattdessen den Vorgang **Container anhalten** auszuwählen.
Images untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Images. Wenn das Kontrollkästchen aktiviert ist, können Sie einen Namen oder eine Namensmaske für Images angeben, die untersucht werden sollen. Das Kontrollkästchen ist standardmäßig aktiviert.
Namensmaske	Eingabefeld für den Namen oder die Maske, welche die zu untersuchenden Images definiert.

	Standardmäßig ist die Maske * angegeben (alle Images werden untersucht).
Aktion beim Erkennen einer Bedrohung	Sie können eine Aktion auswählen, die von der App beim Fund eines infizierten Objekts für das Image ausgeführt werden soll: • **Image überspringen** (Standardwert) – Keine Aktion für das Image ausführen, wenn ein infiziertes Objekt erkannt wird. • **Image löschen**, wenn ein infiziertes Objekt erkannt wird (nicht empfohlen). Alle Abhängigkeiten werden ebenfalls gelöscht. Laufende Container werden angehalten und anschließend gelöscht.
Jede Ebene untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung aller Schichten von Abbildern und gestarteten Containern. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Abschnitt "Ausschlussbereiche"

Im Abschnitt **Ausschlussbereiche** der Aufgabe "Untersuchung von Containern" können Sie die Ausschlüsse nach Maske und nach Bedrohungsnamen sowie die Verwendung globaler Ausnahmen während der Aufgabenausführung konfigurieren.

Einstellungen der Ausschlüsse von der Untersuchung

Einstellung	Beschreibung
Ausschlüsse nach Maske anpassen	Der Link **Ausschlüsse nach Maske anpassen** öffnet das Fenster **Ausschlüsse nach Maske**. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren.
Ausschlüsse nach Bedrohungsname anpassen	Der Link **Ausschlüsse nach Bedrohungsname anpassen** öffnet das Fenster **Ausschlüsse nach Bedrohungsname**. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren.
Globale Ausnahmen verwenden	Das Kontrollkästchen aktiviert oder deaktiviert den Ausschluss von in den globalen Ausnahmen angegeben Mountpunkten während der App-Ausführung. Wenn diese Option aktiviert ist, schließt die App die konfigurierten Mountpunkte von der Untersuchung aus. Das Kontrollkästchen ist standardmäßig aktiviert.

Fenster "Ausschlüsse nach Maske"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren. Die App untersucht keine Dateien, deren Namen die angegebenen Masken enthalten. Standardmäßig ist die Liste mit Masken leer.

Sie können Masken hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist.

Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Bedrohungsname"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren. Die App blockiert die angegebenen Bedrohungen nicht. Standardmäßig ist die Liste mit den Namen von Bedrohungen leer.

Sie können Namen von Bedrohungen hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Bedrohung aus den Ausschlüsse.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens ein Bedrohungsname ausgewählt ist.

Ein Klick auf den Namen einer Bedrohung in der Tabelle öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung ändern, die von der Untersuchung ausgenommen wird.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung angeben, die von der Untersuchung ausgenommen wird.

Untersuchung von Containern in der Verwaltungskonsole

In der Verwaltungskonsole können Sie Container und Images mithilfe der Aufgabe *Untersuchung von Containern* untersuchen.

Sie können Benutzeraufgaben für die Container-Untersuchung erstellen und starten. Sie können die Untersuchungseinstellungen konfigurieren, indem Sie die Aufgabeneinstellungen ändern.

Im Abschnitt **Einstellungen** in den Eigenschaften der Aufgabe "Untersuchung von Containern" können Sie die in der folgenden Tabelle aufgeführten Einstellungen konfigurieren.

Einstellungen der Aufgabe zur Untersuchung von Containern

Einstellung	Beschreibung
Untersuchung	Diese Einstellungsgruppe enthält Schaltflächen, mit denen Fenster geöffnet werden können, in denen Sie die Einstellungen für die Untersuchung von Containern und die allgemeinen Untersuchungseinstellungen anpassen können.
Aktion beim Erkennen einer Bedrohung	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, mit der das Fenster **Aktion beim Erkennen von Bedrohungen** geöffnet werden kann. In diesem Fenster können Sie die Aktionen konfigurieren, die von der App für das erkannte infizierte Objekt ausgeführt werden soll.

Im Abschnitt **Ausschlüsse** können Sie in den Eigenschaften der Aufgabe zur Untersuchung von Containern auch Ausschlüsse Nach Maske und Nach Bedrohungsname konfigurieren.

Fenster "Einstellungen der Container-Untersuchung"

In diesem Fenster können Sie die Einstellungen für die Untersuchung von Containern und Images anpassen.

Einstellungen für die Untersuchung von Containern und Images

Einstellung	Beschreibung
Container untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Containern. Wenn das Kontrollkästchen aktiviert ist, können Sie einen Namen oder eine Namensmaske für Container angeben, die untersucht werden sollen. Das Kontrollkästchen ist standardmäßig aktiviert.
Namensmaske	Eingabefeld für den Namen oder die Maske, welche die zu untersuchenden Container definiert. Standardmäßig ist die Maske * angegeben (alle Container werden untersucht).
Aktion beim Erkennen einer Bedrohung	In dieser Dropdown-Liste können Sie eine Aktion auswählen, die von der App beim Fund eines infizierten Objekts für den Container ausgeführt werden soll: • **Container überspringen** – Keine Aktion für den Container ausführen, wenn ein infiziertes Objekt erkannt wird. • **Container anhalten** – Hält den Container an, wenn ein infiziertes Objekt erkannt wird. • **Anhalten, falls Desinfektion fehlschlägt** (Standardwert) – Hält den Container an, wenn die Desinfektion eines infizierten Objekts fehlgeschlagen ist oder die Bedrohung nicht beseitigt werden konnte. Aufgrund von Besonderheiten der Funktionsweise von CRI-O-Umgebungen werden infizierte Objekte in den Containern einer CRI-O-Umgebung weder desinfiziert noch gelöscht. Es wird daher empfohlen, stattdessen den Vorgang **Container anhalten** auszuwählen.

Images untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Images. Wenn das Kontrollkästchen aktiviert ist, können Sie einen Namen oder eine Namensmaske für Images angeben, die untersucht werden sollen. Das Kontrollkästchen ist standardmäßig aktiviert.
Namensmaske	Eingabefeld für den Namen oder die Maske, welche die zu untersuchenden Images definiert. Standardmäßig ist die Maske * angegeben (alle Images werden untersucht).
Aktion beim Erkennen einer Bedrohung	In dieser Dropdown-Liste können Sie eine Aktion auswählen, die von der App beim Fund eines infizierten Objekts für das Image ausgeführt werden soll: • **Image überspringen** (Standardwert) – Keine Aktion für das Image ausführen, wenn ein infiziertes Objekt erkannt wird. • **Image löschen**, wenn ein infiziertes Objekt erkannt wird (nicht empfohlen). Alle Abhängigkeiten werden ebenfalls gelöscht. Laufende Container werden angehalten und anschließend gelöscht.
Jede Ebene untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung aller Schichten von Abbildern und gestarteten Containern. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Fenster "Untersuchungseinstellungen"

In diesem Fenster können Sie die Einstellungen für die Untersuchung von Dateien durch die Aufgabe konfigurieren.

Untersuchungseinstellungen

Einstellung	Beschreibung
Archive untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Archiven. Wenn das Kontrollkästchen aktiviert ist, so untersucht die App Archive. Um ein Archiv zu untersuchen, muss es zunächst von der App entpackt werden, was die Untersuchung verlangsamen kann. Sie können die Dauer der Untersuchung von Archiven reduzieren, indem Sie im Abschnitt **Allgemeine Untersuchungseinstellungen** die Einstellungen **Dateien überspringen, deren Untersuchung länger dauert als (Sek.)** und/oder **Dateien überspringen, die größer sind als (MB)** konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Archive. Das Kontrollkästchen ist standardmäßig aktiviert.
Selbstentpackende Archive untersuchen	Das Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung *selbstentpackender Archive (self-extracting archives)*. Selbstentpackende Archive sind Archive, die ein ausführbares Modul zum Entpacken enthalten. Wenn das Kontrollkästchen aktiviert ist, untersucht die App selbstentpackende Archive. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine selbstentpackenden Dateien. Dieses Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Archive untersuchen** deaktiviert ist. Das Kontrollkästchen ist standardmäßig aktiviert.
Mail-Datenbanken	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Mail-

untersuchen	Datenbanken der Anwendungen Microsoft Outlook, Outlook Express, The Bat! und anderen E-Mail-Clients. Wenn das Kontrollkästchen aktiviert ist, untersucht die App die Dateien von Mail-Datenbanken. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App keine Dateien von Mail-Datenbanken. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Dateien in Mail-Formaten untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Dateien von E-Mail-Nachrichten im Textformat (plain text). Wenn das Kontrollkästchen aktiviert ist, untersucht die App E-Mail-Nachrichten im Textformat. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App E-Mail-Nachrichten im Textformat nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Dateien überspringen, deren Untersuchung länger dauert als (Sek.)	In diesem Feld können Sie die erlaubte Höchstdauer für die Untersuchung der Datei in Sekunden angeben. Nach Ablauf des angegebenen Zeitraums bricht die App die Untersuchung der Datei ab. Zulässige Werte: 0–9999. Ist der Wert 0 angegeben, dann ist die Untersuchungsdauer nicht beschränkt. Standardwert: 0.
Dateien überspringen, die größer sind als (MB)	In diesem Feld können Sie die maximale Größe der untersuchten Datei in Megabyte angeben. Zulässige Werte: 0–999999. Ist der Wert 0 angegeben, untersucht die App Dateien jeder Größe. Standardwert: 0.
Virenfreie Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectProcessed*. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Unverarbeitete Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectNotProcessed*, wenn eine Datei während der Untersuchung nicht verarbeitet werden kann. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *ObjectNotProcessed*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *ObjectNotProcessed*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Gepackte Objekte protokollieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Protokollierung der Ereignisse vom Typ *PackedObjectDetected* für alle erkannten gepackten Objekte. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App Ereignisse vom Typ *PackedObjectDetected*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App keine Ereignisse vom Typ *PackedObjectDetected*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
iChecker-	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung nur neuer oder

Technologie verwenden	seit der letzten Untersuchung geänderter Dateien. Wenn das Kontrollkästchen aktiviert ist, untersucht die App nur neue oder seit der letzten Untersuchung geänderte Dateien. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App Dateien unabhängig von ihrem Erstellungs- oder Änderungsdatum. Das Kontrollkästchen ist standardmäßig aktiviert.
Heuristische Analyse verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die heuristische Analyse bei der Untersuchung von Dateien. Das Kontrollkästchen ist standardmäßig aktiviert.
Stufe der heuristischen Analyse	Wenn das Kontrollkästchen **Heuristische Analyse verwenden** aktiviert ist, können Sie die Ebene der heuristischen Analyse in der Dropdown-Liste festlegen: • **Oberflächlich** – Die am wenigsten detaillierte Untersuchung, minimale Systembelastung. • **Mittel** – Mittlere Untersuchung, ausgeglichene Systembelastung. • **Tief** – Detaillierteste Untersuchung, maximale Systembelastung. • **Empfohlen** (Standardwert) – Optimale Stufe, die von den Kaspersky-Experten empfohlen wird. Sie bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Geräte.

•

Fenster "Aktion beim Fund einer Bedrohung"

In diesem Fenster können Sie Aktionen auswählen, die von der App Kaspersky Endpoint Security für gefundene infizierte Objekte ausgeführt werden soll.

Aktionen beim Fund einer Bedrohung

Einstellung	Beschreibung
Erste Aktion	In der Dropdown-Liste können Sie die erste Aktion auswählen, die von der App für das gefundene infizierte Objekt ausgeführt werden soll: • Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Informationen zur Gefahrenstufe der in der Datei erkannten Bedrohung und zur Möglichkeit ihrer Desinfektion (Standardwert). • Objekt **überspringen**.
Zweite Aktion	In dieser Dropdown-Liste können Sie die zweite Aktion auswählen, die von der App für ein infiziertes Objekt ausgeführt werden soll, falls die erste Aktion nicht erfolgreich war: • Objekt **desinfizieren**. Eine Kopie des infizierten Objekts wird im Backup abgelegt. • Objekt **löschen**. Eine Kopie des infizierten Objekts wird im Backup abgelegt.

	• Für das Objekt die **Empfohlene Aktion ausführen**, basierend auf Daten zur in der Datei erkannten Gefahrenstufe der Bedrohung und zur Möglichkeit ihrer Desinfektion. • Objekt **überspringen** (Standardwert).

•

Abschnitt "Ausschlüsse"

Einstellungen der Ausschlüsse von der Untersuchung

Einstellungsgruppe	Beschreibung
Ausschlüsse nach Maske	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausschlüsse nach Maske** öffnet. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren.
Ausschlüsse nach Bedrohungsname	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausschlüsse nach Bedrohungsname** öffnet. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren.
Globale Ausnahmen verwenden	Das Kontrollkästchen aktiviert oder deaktiviert den Ausschluss von in den globalen Ausnahmen angegeben Mountpunkten während der App-Ausführung. Wenn diese Option aktiviert ist, schließt die App die konfigurierten Mountpunkte von der Untersuchung aus. Das Kontrollkästchen ist standardmäßig aktiviert.

Fenster "Ausschlüsse nach Maske"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren. Die App untersucht keine Dateien, deren Namen die angegebenen Masken enthalten. Standardmäßig ist die Liste mit Masken leer.

Sie können Masken hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist.

Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Bedrohungsname"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren. Die App blockiert die angegebenen Bedrohungen nicht. Standardmäßig ist die Liste mit den Namen von Bedrohungen leer.

Sie können Namen von Bedrohungen hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Bedrohung aus den Ausschlüsse.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens ein Bedrohungsname ausgewählt ist.

Ein Klick auf den Namen einer Bedrohung in der Tabelle öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung ändern, die von der Untersuchung ausgenommen wird.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung angeben, die von der Untersuchung ausgenommen wird.

Untersuchung von Containern über die Befehlszeile

Über die Befehlszeile können Sie die Untersuchung von Containern und Images auf folgende Arten durchführen:

- Mithilfe der vordefinierten Aufgabe Untersuchung von Containern (*Container_Scan*). Sie können diese Aufgabe manuell starten und beenden und den Zeitplan für den Aufgabenstart konfigurieren. Sie können die Einstellungen für die Untersuchung konfigurieren, indem Sie die Einstellungen für diese Aufgabe ändern.
- Mithilfe von Benutzeraufgaben zur Container-Untersuchung (Aufgaben vom Typ *ContainerScan*). Sie können Benutzeraufgaben manuell starten und beenden und den Zeitplan für den Aufgabenstart konfigurieren.
- Mit dem Befehl `kesl-control --scan-container` können Sie eine *benutzerdefinierte Untersuchung* bestimmter Container und Images durchführen.

Einstellungen der Aufgabe zur Untersuchung von Containern

Alle verfügbaren Werte und Standardwerte für jede Einstellung der Untersuchung von Containern und Images werden in der nachstehenden Tabelle beschrieben.

Einstellungen der Aufgabe zur Untersuchung von Containern

Einstellung	Beschreibung	Werte
`ScanContainers`	Untersuchung von Containern, die mittels Maske spezifiziert werden. Sie können Masken mit dem Parameter `ContainerNameMask` angeben.	`Yes` (Standardwert) – Die mittels Maske angegebenen Container untersuchen. `No` – Die mittels Maske angegebenen Container nicht untersuchen.

`ContainerNameMask`	Legt einen Namen oder eine Namensmaske fest, die den zu untersuchenden Container definiert.
	Masken werden im Format der Befehlsschnittstelle angegeben. Sie können die folgenden Symbole verwenden: "?" und "*".
	Bevor Sie diese Einstellung angeben, stellen Sie sicher, dass für die Einstellung der Wert `ScanContainers=Yes` angegeben ist.
		Der Standardwert ist "*" (alle Container untersuchen).
		Beispiele:
		So untersuchen Sie einen Container mit dem Namen my_container:
		`ContainerNameMask=my_container`
		So untersuchen Sie alle Container, deren Namen mit my_container beginnen:
		`ContainerNameMask=my_container*`
		So untersuchen Sie alle Container, deren Namen mit my_ beginnen, dann fünf beliebige Zeichen enthalten und anschließend von _container und einer beliebigen Zeichenfolge gefolgt sind:
		`ContainerNameMask=my_?????_container*`

`ScanImages`	Untersuchung der Images, die mittels Maske spezifiziert werden. Sie können Masken mit dem Parameter `ImageNameMask` angeben.	`Yes` (Standardwert) – Die anhand der Maske festgelegten Images untersuchen. `No` – Die anhand der Maske festgelegten Images nicht untersuchen.

`ImageNameMask`	Legt einen Namen oder eine Namensmaske fest, welche die zu untersuchenden Images definiert.
	Bevor Sie diese Einstellung festlegen, überzeugen Sie sich, dass der Wert der Einstellung `ScanImages` auf `Yes` festgelegt ist.
	Masken werden im Format der Befehlsschnittstelle angegeben.
	Wenn Sie mehrere Masken angeben möchten, muss jede Maske in einer neuen Zeile mit einem neuen Index angegeben werden.
		Der Standardwert ist "*" (alle Images untersuchen).
		Beispiele:
		So untersuchen Sie ein Image mit dem Namen "my_image" und dem Tag-Wert "latest":
		`ImageNameMask=my_image:latest`
		So untersuchen Sie alle Images, deren Namen mit "my_image_" beginnen und die einen beliebigen Tag-Wert haben:
		`ImageNameMask=my_image*`

`DeepScan`	Untersuchung aller Image-Ebenen und gestarteten Container.	`Yes` – Alle Ebenen untersuchen. `No` (Standardwert) – Nicht alle Ebenen untersuchen.
`ContainerScanAction`	Aktion, die für einen Container ausgeführt werden soll, wenn ein infiziertes Objekt erkannt wird. Die Aktionen für infizierte Objekte in einem Container werden nachfolgend beschrieben.	`StopContainerIfFailed` (Standardwert) – Die App hält den Container an, falls die Desinfektion oder das Löschen eines infizierten Objekts fehlschlägt. Aufgrund von Besonderheiten der Funktionsweise von CRI-O-Umgebungen werden infizierte Objekte in den Containern einer CRI-O-Umgebung weder desinfiziert noch gelöscht. Es wird stattdessen empfohlen, den Vorgang `StopContainer` auszuwählen. `StopContainer` – Die App hält den Container an, wenn ein infiziertes Objekt erkannt wird. `Skip` – Die App führt keine Aktion für Container aus, wenn ein infiziertes Objekt erkannt wird.
`ImageAction`	Legt die Aktion fest, die für ein Image ausgeführt werden soll, wenn ein infiziertes Objekt erkannt wird. Die Aktionen für infizierte Objekte in einem Image werden nachfolgend beschrieben.	`Skip` (Standardwert) – Die App führt keine Aktion für das Image aus, wenn ein infiziertes Objekt erkannt wird. `Delete` – Die App löscht das Image, wenn ein infiziertes Objekt erkannt wird (nicht empfohlen). Alle Abhängigkeiten werden ebenfalls gelöscht. Laufende Container werden angehalten und anschließend gelöscht.

Nachfolgend werden die Einstellungen beschrieben, die auf Objekte innerhalb von Containern und Images angewendet werden.

Einstellungen der Aufgabe zur Untersuchung von Containern

Einstellung	Beschreibung	Werte
`ScanArchived`	Aktiviert die Untersuchung von Archiven (einschließlich selbstentpackender sfx-Archive). Die App untersucht Archive wie .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. Die Liste der unterstützten Archivformate hängt von den verwendeten App-Datenbanken ab.	`Yes` (Standardwert) – Archive untersuche Wenn der Wert `FirstAction=Recommended` angegeben ist, löscht die App je nach Archivtyp entweder das infizierte Objekt oder das gesamte Archiv, das die Bedrohung enthält `No` – Archive nicht untersuchen.
`ScanSfxArchived`	Aktiviert die Untersuchung von	`Yes` (Standardwert) – Selbstentpackende

	nur selbstentpackenden Archiven (Archiven, zu deren Bestandteilen ein ausführbares Dekompressionsmodul gehört).	Archive untersuchen. `No` – Selbstentpackende Archive nicht untersuchen.
`ScanMailBases`	Aktiviert die Untersuchung von E-Mail-Datenbanken von Microsoft Outlook, Outlook Express, The Bat und anderer Mail-Clients.	`Yes` – Dateien von E-Mail-Datenbanken untersuchen. `No` (Standardwert) – Dateien von E-Mail-Datenbanken nicht untersuchen.
`ScanPlainMail`	Aktiviert die Untersuchung von E-Mail-Nachrichten im Textformat (plain text).	`Yes` – E-Mail-Nachrichten im Textformat untersuchen. `No` (Standardwert) – E-Mail-Nachrichten in Textformat nicht untersuchen.
`TimeLimit`	Maximale Untersuchungsdauer (in Sekunden) eines Objekts. Die App stellt die Untersuchung eines Objekts ein, wenn sie länger dauert als durch diese Einstellung festgelegt.	0 – 9999 0 – die Untersuchungsdauer für Objekte ist nicht begrenzt. Standardwert: 0.
`SizeLimit`	Maximale Größe des zu untersuchenden Objekts (in Megabyte). Wenn die Größe des zu untersuchenden Objekts den angegebenen Wert überschreitet, überspringt die App das Objekt während der Untersuchung.	0 – 999999 0 – Die App untersucht Objekte beliebiger Größe. Standardwert: 0.
`FirstAction`	Auswahl der ersten Aktion, welche die App für infizierte Objekte ausführen soll.	`Disinfect` (desinfizieren) – Die App versucht, ein Objekt zu desinfizieren, und speichert eine Kopie davon im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder der Typ der Bedrohung im Objekt nicht desinfiziert werden kann), belässt die App das Objekt unverändert. Wenn die erste Aktion auf `Desinfizieren` festgelegt ist, wird empfohlen, die zweite Aktion mithilfe der Einstellung `SecondAction` anzugeben. `Remove` (löschen) – Die App löscht das infizierte Objekt, nachdem eine Backup-Kopie davon erstellt wurde. `Recommended` (empfohlene Aktion ausführen) – Die App wählt automatisch eine Aktion für das Objekt und führt sie aus, wobei Informationen zu der im Objekt gefundenen Bedrohung berücksichtigt werden. Beispielsweise löscht Kaspersky Endpoint Security Trojaner sofort, da sie andere Dateien nicht infizieren und deshalb keine Desinfektion erfordern. `Skip` (überspringen) – Die App unternimmt keinen Versuch, das infizierte Objekt zu desinfizieren oder zu löschen. Informationen über das infizierte Objekt werden im Protokoll gespeichert.

		Standardwert: `Recommended`
`SecondAction`	Auswahl der zweiten Aktion, welche die App für infizierte Objekte ausführen soll. Die App führt die zweite Aktion aus, wenn die Ausführung der ersten Aktion misslingt.	Die Werte der Einstellung `SecondAction` sind dieselben wie die Werte der Einstellun `FirstAction`. Wenn als erste Aktion `Skip` oder `Remove` ausgewählt ist, muss keine zweite Aktion angegeben werden. In allen anderen Fällen wird empfohlen, zwei Aktionen anzugeben. Wenn Sie keine zweite Aktion angegeben haben, wendet die App `Skip` (überspringe als zweite Aktion an. Standardwert: `Skip`
`UseExcludeMasks`	Steuert den Ausschluss von Objekten, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, aus der Untersuchung.	`Yes` – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, aus der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht aus der Untersuchur ausschließen.

`ExcludeMasks.item_#`	Ausschluss von der Untersuchung von Objekten nach Name oder Maske. Mit dieser Einstellung können Sie eine einzelne Datei anhand des Namens oder mehrere Dateien anhand von Masken im Shell-Format aus dem angegebenen Untersuchungsbereich ausschließen.	Der Standardwert ist nicht angegeben.
		Beispiel:
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Steuert den Ausschluss von Objekten mit Bedrohungen, die durch die Einstellung `ExcludeThreats.item_#` festgelegt sind, aus der Untersuchung.	`Yes` – Objekte, die Bedrohungen enthalter die in der Einstellung `ExcludeThreats.item_#` angegeben sin von der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die Bedrohungen enthalten, die in der Einstellung `ExcludeThreats.item_#` angegeben sind, nicht von der Untersuchur ausschließen.

`ExcludeThreats.item_#`	Schließt Objekte nach dem Namen der in den Objekten gefundenen Bedrohungen von der Untersuchung aus. Bevor Sie die Werte dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseExcludeThreats` aktiviert ist.	Beim Wert der Einstellung muss die Groß- und Kleinschreibung beachtet werden.
		Der Standardwert ist nicht angegeben.
		Beispiel:
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

	Um ein Objekt von der Untersuchung auszuschließen, geben Sie den vollständigen Namen der Bedrohung an, die im Objekt gefunden wurde, d. h. die Zeile mit der Entscheidung der App, dass dieses Objekt infiziert ist. Sie können beispielsweise ein Tool zum Sammeln von Informationen über Ihr Netzwerk verwenden. Damit es von der App nicht blockiert wird, fügen Sie den vollständigen Namen der darin enthaltenen Bedrohung zur Liste der Bedrohungen hinzu, die von der Untersuchung ausgenommen sind. Den vollständigen Namen der im Objekt gefundenen Bedrohung finden Sie im Protokoll der App oder auf der Website https://threats.kaspersky.com.	
`UseGlobalExclusions`	Aktivieren der Verwendung von globalen Ausnahmen während der Untersuchung.	`Yes` (Standardwert) – Globale Ausnahmen verwenden. `No` – Keine globale Ausnahmen verwenden
`ReportCleanObjects`	Aktiviert die Protokollierung von Informationen zu untersuchten Objekten, welche die App als nicht infiziert einstuft. Sie können diese Einstellung aktivieren, um beispielsweise sicherzustellen, dass ein bestimmtes Objekt durch die App untersucht wurde.	`Yes` – Informationen zu nicht infizierten Objekten im Protokoll speichern. `No` (Standardwert) – Informationen zu nicht infizierten Objekten nicht im Protokoll speichern.
`ReportPackedObjects`	Aktiviert das Protokollieren von Informationen über untersuchte Objekte, die Bestandteil zusammengesetzter Objekte sind. Sie können diese Einstellung aktivieren, um beispielsweise sicherzustellen, dass ein bestimmtes Objekt innerhalb eines Archivs von der App untersucht wurde.	`Yes` – Informationen über die Untersuchung von Objekten, die zu einem Archiv gehören, im Protokoll speichern. `No` (Standardwert) – Informationen über die Untersuchung von Objekten, die zu einem Archiv gehören, nicht im Protokoll speichern
`ReportUnprocessedObjects`	Aktiviert das Protokollieren von Informationen über Objekte, die aus einem bestimmten Grund nicht verarbeitet wurden.	`Yes` – Informationen zu nicht verarbeiteten Objekten im Protokoll speichern. `No` (Standardwert) – Informationen zu nicht verarbeiteten Objekten nicht im Protokoll speichern.
`UseAnalyzer`	Aktiviert die heuristische Analyse.	`Yes` (Standardwert) – Heuristische Analyse aktivieren.

	Mithilfe der heuristischen Analyse kann die App Bedrohungen bereits erkennen, bevor sie den Virenanalysten bekannt sind.	`No` – Heuristische Analyse deaktivieren.
`HeuristicLevel`	Legt die Stufe der heuristischen Analyse fest. Sie können die Ebene der heuristischen Analyse festlegen. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Gründlichkeit der Suche nach Bedrohungen, der Belastung der Betriebssystemressourcen und der Untersuchungsdauer. Je höher die festgelegte Ebene der heuristischen Analyse, desto mehr Ressourcen verbraucht die Untersuchung und desto länger dauert sie.	`Light` – Oberflächlichste Untersuchung m minimaler Belastung des Systems. `Medium` – Mittlere Ebene der heuristischer Analyse mit ausgeglichener Belastung des Betriebssystems. `Deep` – Gründlichste Untersuchung mit maximaler Belastung des Betriebssystems. `Recommended` (Standardwert) – Der empfohlene Wert.
`UseIChecker`	Aktiviert die Nutzung der iChecker-Technologie.	`Yes` (Standardwert) – Nutzung der iChecker-Technologie aktivieren. `No` – Nutzung der iChecker-Technologie deaktivieren.

Benutzerdefinierte Untersuchung von Containern und Images

Mit dem Befehl `kesl-control --scan-container` können Sie eine benutzerdefinierte Untersuchung bestimmter Container und Images durchführen.

Eine benutzerdefinierte Untersuchung wird mit Einstellungen durchgeführt, die in der vordefinierten Aufgabe *Custom_Container_Scan* (ID:19) gespeichert sind. Sie können die Einstellungen für die benutzerdefinierte Untersuchung von Containern und Images konfigurieren, indem Sie die Einstellungen für diese Aufgabe ändern. Standardmäßig hat die Aufgabe *Custom_Container_Scan* dieselben Einstellungen wie die Aufgabe *Container_Scan* (ID:18).

Um eine erneute benutzerdefinierte Untersuchung von Containern zu starten, führen Sie den folgenden Befehl aus:

```
kesl-control --scan-container <Container/Image [:tag]>
```

Wobei gilt: `<Container/Image [:tag]>` – Name oder ID des Containers oder Images. Um mehrere Objekte zu untersuchen, können Sie Masken verwenden.

Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Bei mehreren Entitäten mit demselben Namen untersucht die App alle Entitäten.

Als Ergebnis der Ausführung des Befehls wird eine temporäre Aufgabe zur Untersuchung von Containern und Images erstellt, die nach Abschluss automatisch gelöscht wird. Gleichzeitig werden die Ergebnisse der Untersuchung in die Konsole ausgegeben.

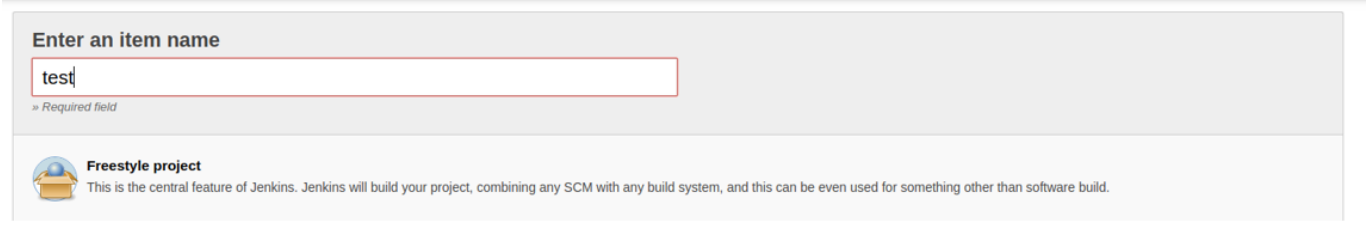
Beispiele:
Untersucht einen Container mit dem Namen my_container:
```
kesl-control --scan-container my_container
```
Untersucht ein Image namens "my_image" (alle Tags):
```
kesl-control --scan-container my_image*
```

Integration mit Jenkins

Kaspersky Endpoint Security unterstützt die Integration mit Jenkins. Plug-ins für Jenkins Pipeline können auf verschiedenen Etappen zur Untersuchung von Docker-Images verwendet werden. So können Sie z. B. Docker-Images in einem Repository während des Entwicklungsprozesses oder vor der Veröffentlichung untersuchen.

So integrieren Sie Kaspersky Endpoint Security in Jenkins:

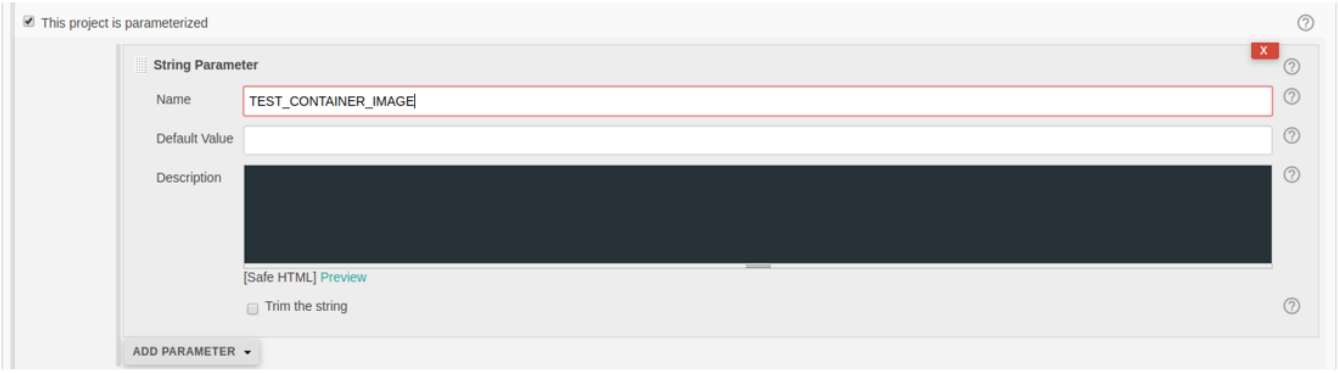
1. Installieren Sie Kaspersky Endpoint Security auf einem Jenkins-Node.
2. Installieren Sie Docker Engine auf einem Jenkins-Node.
   Weitere Informationen finden Sie in der Dokumentation zu Docker Engine.
3. Gewähren Sie dem Nutzer "Jenkins" folgende Administrator-Berechtigungen für Kaspersky Endpoint Security:
   ```
   kesl-control --grant-role admin <Jenkins-Nutzername>
   ```
4. Fügen Sie der Gruppe "docker" einen Jenkins-Benutzer hinzu:
   ```
   sudo usermod -aG docker <Jenkins-Benutzername>
   ```
   Normalerweise wird der Name "jenkins" verwendet.
5. Erstellen Sie in Jenkins eine neue Build-Aufgabe mit dem Namen `test` (**New Item** → **Enter an item name**).



6. Konfigurieren Sie das Projekt nach Ihren Bedürfnissen. Es wird davon ausgegangen, dass Sie in Folge dessen über ein Image oder einen gestarteten Container verfügen, dass Sie untersuchen müssen.

7. Um den Docker-Container zu starten, fügen Sie der Jenkins Build-Prozedur folgendes Skript an. Wenn Sie Jenkins Plug-ins oder andere Werkzeuge verwenden, um Docker-Container zu starten, speichern Sie die ID des ausgeführten Docker-Containers zur weiteren Untersuchung in der Datei /tmp/kesl_cs_info:

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
echo "Start container from image: '${TEST_CONTAINER_IMAGE}'"
CONTAINER_ID=$(docker run -d -v /storage:/storage ${TEST_CONTAINER_IMAGE}
/storage/docker_process.sh)
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot start container from image ${TEST_CONTAINER_IMAGE}"
exit 1
fi
echo "${CONTAINER_ID}" > ${TMP_FILE}
exit ${EXIT_CODE}
```



8. Nachdem die Artefakte gebaut wurden, fügen Sie den Schritten das folgende Skript hinzu, um Jenkins zu bauen.

   Dieses Skript unterstützt einen zu untersuchenden Container. Bei Bedarf können Sie das Skript Ihren Bedürfnissen anpassen.

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
if [ ! -f "${TMP_FILE}" ] ; then
echo "Cannot find temporary file with container ID: '${TMP_FILE}'"
exit 1
fi
CONTAINER_ID=$(cat ${TMP_FILE})
if [ -z "${CONTAINER_ID}" ] ; then
```

```
echo "Cannot find container ID in the temporary file: '${TMP_FILE}'"
exit 1
fi
echo "Start anti-virus scan for: '${CONTAINER_ID}'"
THREATS_AMOUNT=$(kesl-control --scan-container ${CONTAINER_ID}|grep 'Total detected objects'|awk '{print $5}')
if [ "${THREATS_AMOUNT}" != "0" ] ; then
echo "ATTENTION! ${THREATS_AMOUNT} threats detected at: '${CONTAINER_ID}'"
EXIT_CODE=1
else
echo "Not threats found"
fi
echo "Remove container: {${CONTAINER_ID}}"
docker kill ${CONTAINER_ID}
docker rm -f ${CONTAINER_ID}
rm -f ${TMP_FILE}
```

9. Verwenden Sie das folgende Skript, um ein Docker-Image aus einem Repository zu untersuchen:

```
DOCKER_FILE=https://raw.githubusercontent.com/ianmiell/simple-dockerfile/master/Dockerfile
DOCKER_FILE_FETCHED=$$.Dockerfile
TEST_IMAGE_NAME=test_image
echo "Build image from ${DOCKER_FILE}"
curl ${DOCKER_FILE} -o ${DOCKER_FILE_FETCHED}
if [ -f ${DOCKER_FILE_FETCHED} ] ; then
echo "Dockerfile fetched: ${DOCKER_FILE_FETCHED}"
else
echo "Dockerfile not fetched"
exit 1
fi
docker build -f ${DOCKER_FILE_FETCHED} -t ${TEST_IMAGE_NAME}
echo "Scan docker image"
SCAN_RESULT=$(/opt/kaspersky/kesl/bin/kesl-control --scan-container ${TEST_IMAGE_NAME}*)
echo "Scan done: "
echo $SCAN_RESULT
```

10. Speichern Sie die Build-Aufgabe.

Firewall-Verwaltung

Bei der Verwendung von lokalen Netzwerken und des Internets ist ein Gerät neben Viren und anderer Schadsoftware auch einer Vielzahl von Angriffen ausgesetzt, die Schwachstellen in Betriebssystemen und Software ausnutzen. Die Firewall des Betriebssystems schützt die auf dem Gerät des Benutzers gespeicherten persönlichen Daten, indem sie die meisten Bedrohungen für das Betriebssystem blockiert, wenn das Gerät mit dem Internet oder einem lokalen Netzwerk verbunden ist.

Mit der Betriebssystem-Firewall können Sie alle Netzwerkverbindungen auf dem Gerät des Benutzers erkennen und eine Liste seiner IP-Adressen bereitstellen. Mit der Komponente "Firewall-Verwaltung" können Sie den Status dieser Netzwerkverbindungen festlegen, indem Sie Netzwerkpaketregeln konfigurieren.

Diese Funktionalität wird im KESL-Container nicht unterstützt.

Mithilfe von Netzwerkpaketregeln können Sie die gewünschte Ebene des Geräteschutzes von der Blockierung des Internetzugangs für alle Apps bis zur Erlaubnis von unbegrenztem Zugang festlegen. Alle ausgehenden Verbindungen werden standardmäßig erlaubt, sofern keine entsprechende Verbotsregeln für die Komponente "Firewall-Verwaltung" angegeben sind.

Standardmäßig ist die Komponente "Firewall-Verwaltung" deaktiviert.

Es wird empfohlen, vor der Aktivierung der Komponente "Firewall-Verwaltung" andere Tools zur Verwaltung der betriebssystemeigenen Firewall zu deaktivieren.

Wenn Sie die Komponente "Firewall-Verwaltung" aktivieren, löscht Kaspersky Endpoint Security automatisch alle Benutzerregeln, die für die Firewall mithilfe des Betriebssystems konfiguriert wurden. Nach dem Deaktivieren der Komponente werden diese Regeln nicht wiederhergestellt. Speichern Sie bei Bedarf benutzerdefinierte Firewall-Regeln, bevor Sie die Komponente "Firewall-Verwaltung" aktivieren.

Wenn die Firewall-Verwaltung aktiviert ist, untersucht Kaspersky Endpoint Security die Firewall des Betriebssystems und blockiert jeden Versuch, die Firewall-Einstellungen zu ändern, beispielsweise wenn eine Anwendung oder ein Tool versucht, eine Firewall-Regel hinzuzufügen oder zu entfernen. Kaspersky Endpoint Security überprüft die Firewall des Betriebssystems alle 60 Sekunden und stellt bei Bedarf die mithilfe der App erstellten Firewall-Regeln wieder her. Das Überprüfungsintervall kann nicht geändert werden.

In den Betriebssystemen Red Hat Enterprise Linux und CentOS 8 können Firewall-Regeln, die mit Kaspersky Endpoint Security erstellt wurden, nur mithilfe von Verwaltungsbefehlen angezeigt werden (Befehl `kesl-control -F --query`).

Kaspersky Endpoint Security überprüft weiterhin die Firewall des Betriebssystems, selbst wenn die Firewall-Verwaltung deaktiviert ist. Das ermöglicht der App, die dynamischen Regeln wiederherzustellen.

Sie können die Firewall-Verwaltung aktivieren und deaktivieren und auch die folgenden Einstellungen konfigurieren:

- Konfigurieren Sie eine Liste von Netzwerkpaketregeln, die Kaspersky Endpoint Security anwenden soll, wenn es einen Versuch erkennt, eine Netzwerkverbindung herzustellen. Sie können Netzwerkpaketregeln hinzufügen und entfernen sowie die Ausführungspriorität einer Netzwerkpaketregel ändern
- Wählen Sie Standardaktionen aus, die mit eingehenden Verbindungen oder Paketen ausgeführt werden sollen, wenn für diese Verbindungsart keine anderen Netzwerkpaketregeln angewendet werden können.

- Legen Sie Netzwerkadressen so fest, dass sie vordefinierten Netzwerkzonen entsprechen. Sie können IP-Adressen oder Subnetze zu Netzwerkzonen hinzufügen und Adressen aus Netzwerkzonen entfernen.

- Aktivieren und deaktivieren Sie das automatische Hinzufügen von Erlaubnisregeln für Ports des Administrationsagenten.

Um mögliche Probleme auf Systemen mit "nftables" zu vermeiden, verwendet Kaspersky Endpoint Security beim Hinzufügen von Regeln für die Firewall des Betriebssystems die System-Tools "iptables" und "iptables-restore". Die App erstellt eine spezielle Berechtigungskette für kesl_bypass-Regeln und fügt sie am Beginn der mangle-Liste der Tools iptables und ip6tables hinzu. Mit den Kettenregeln kesl_bypass können Sie Datenverkehr von der Untersuchung durch Kaspersky Endpoint Security ausschließen. Das Ändern der Regeln in dieser Kette wird durch das Betriebssystem durchgeführt. Wenn die App entfernt wird, wird die Regelkette kesl_bypass in iptables und ip6tables nur entfernt, wenn sie leer war.

Über Netzwerkpaketregeln

Netzwerkpaketregeln sind erlaubende oder blockierende Aktionen, die von Kaspersky Endpoint Security ausgeführt werden, wenn eine versuchte Netzwerkverbindung erkannt wird.

Die Regeln legen unabhängig von der App Beschränkungen für Netzwerkpakete fest. Solche Regeln schränken den eingehenden und ausgehenden Netzwerkverkehr durch bestimmte Ports des gewählten Datenprotokolls ein.

Alle ausgehenden Verbindungen werden standardmäßig erlaubt (Standardeinstellung der Aktionen), sofern keine entsprechende Verbotsregeln für die Firewall-Verwaltung angegeben sind. Die Standardaktion wird mit niedrigster Priorität ausgeführt: wenn keine andere Netzwerkpaketregel ausgelöst wurde, oder wenn keine Netzwerkpaketregeln angegeben sind, wird die Verbindung erlaubt.

In der Firewall-Verwaltung sind bestimmte Netzwerkpaketregeln standardmäßig angegeben. Sie können Ihre eigenen Netzwerkpaketregeln erstellen und für jede Netzwerkpaketregel eine Ausführungspriorität festlegen.

Über dynamische Regeln

Mit Kaspersky Endpoint Security können Sie der Firewall *dynamische Regeln*, die für ihren ordnungsgemäßen Betrieb erforderlich sind, hinzufügen oder diese löschen. Beispielsweise fügt der Administrationsagent dynamische Regeln hinzu, die Verbindungen mit Kaspersky Security Center erlauben, die sowohl von der App als auch von Kaspersky Security Center initiiert werden. Die Regeln zum Schutz vor Verschlüsselung sind ebenfalls dynamisch.

Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, werden der Firewall automatisch dynamische Regeln hinzugefügt, die Verbindungen zur SVM und zum Integrationsserver ermöglichen.

Kaspersky Endpoint Security überwacht dynamische Regeln nicht und blockiert den Zugriff auf Netzwerkressourcen für die Komponenten der App nicht. Dynamische Regeln hängen nicht vom Status der Komponente "Firewall-Verwaltung" (gestartet/beendet) oder den Änderungen ihrer Ausführungseinstellungen ab. Die Ausführungspriorität für dynamische Regeln ist höher als die Priorität für Netzwerkpaketregeln. Die App stellt die Auswahl von dynamischen Regeln wieder her, wenn eine davon beispielsweise mithilfe des Tools iptables gelöscht wurde.

Sie können eine Auswahl von dynamischen Regeln (mithilfe des Befehls `kesl-control -F --query`) anzeigen, die Einstellungen der dynamischen Regeln jedoch nicht ändern.

Über die vordefinierten Netzwerkzonennamen

Bei einer *vordefinierten Netzwerkzone* handelt es sich um eine bestimmte Gruppe von IP-Adressen oder Subnetzen. Mit einer vordefinierten Netzwerkzone können Sie dieselben Regeln für mehrere IP-Adressen oder Subnetze verwenden, anstatt separate Regeln für jede IP-Adresse oder jedes Subnetz zu erstellen. Die Netzwerkzone kann beim Erstellen einer Netzwerkpaketregel als Wert für die Einstellung "Remote-Adresse" verwendet werden. Kaspersky Endpoint Security verfügt über drei vordefinierte Netzwerkzonen mit festgelegten Namen:

- **Öffentlich**. Fügen Sie dieser Zone eine Netzwerkadresse oder ein Subnetz hinzu, wenn sie Netzwerken zugewiesen ist, die nicht durch Virenschutzanwendungen, Firewalls oder Filter geschützt sind (z. B. für Netzwerke von Internetcafés).
- **Lokal**. Fügen Sie dieser Zone eine Netzwerkadresse oder ein Subnetz hinzu, wenn sie Netzwerken zugewiesen ist, deren Benutzer berechtigt sind, auf Dateien und Drucker auf diesem Gerät zuzugreifen (z. B. lokale Netzwerke oder Heimnetzwerke).
- **Vertrauenswürdig**. Diese Zone ist für sichere Netzwerke vorgesehen, in denen das Gerät keinen Angriffen oder unbefugten Datenzugriffsversuchen ausgesetzt ist.

Sie können keine Netzwerkzone erstellen oder löschen. IP-Adressen und Subnetze können der Netzwerkzone hinzugefügt oder aus dieser gelöscht werden.

Firewall-Verwaltung in der Web Console

In der Web Console können Sie Einstellungen der Firewall-Verwaltung in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen** → **Basisschutz** → **Firewall-Verwaltung**).

Einstellungen der Komponente "Firewall-Verwaltung"

Einstellung	Beschreibung
Firewall-Verwaltung aktiviert/deaktiviert	Dieser Schalter aktiviert/deaktiviert die Firewall-Verwaltung. Der Schalter ist standardmäßig deaktiviert.
Netzwerkpaketregeln	Der Link **Netzwerkpaketregeln anpassen** öffnet das Fenster **Netzwerkpaketregeln**. In diesem Fenster können Sie eine Liste von Netzwerkpaketregeln konfigurieren, die von der Komponente "Firewall-Verwaltung" angewendet werden, wenn eine versuchte Netzwerkverbindung erkannt wird.
Verfügbare Netzwerke	Der Link **Verfügbare Netzwerke anpassen** öffnet das Fenster **Verfügbare Netzwerke**. In diesem Fenster können Sie eine Liste mit Netzwerken festlegen, die von der Komponente "Firewall-Verwaltung" überwacht werden sollen.
Eingehende Verbindungen	In dieser Dropdown-Liste können Sie eine Aktion auswählen, die für eingehende Netzwerkverbindungen ausgeführt wird: • Netzwerkverbindungen **erlauben** (Standardwert). • Eingehende Netzwerkverbindungen **blockieren**.
Eingehende Pakete	In dieser Dropdown-Liste können Sie eine Aktion auswählen, die für eingehende Pakete ausgeführt wird: • Eingehende Pakete **erlauben** (Standardwert). • Eingehende Pakete **blockieren**.
Erlaubnisregeln für	Dieses Kontrollkästchen aktiviert oder deaktiviert das automatische Hinzufügen

Ports des Administrationsagenten immer hinzufügen	von Erlaubnisregeln für Ports des Administrationsagent. Das Kontrollkästchen ist standardmäßig aktiviert.

Fenster "Regeln für Netzwerkpakete"

Die Tabelle **Netzwerkpaketregeln** enthält Regeln für Netzwerkpakete, die von der Komponente "Firewall-Verwaltung" zur Überwachung der Netzwerkaktivität verwendet werden. Für Netzwerkpaketregeln können Sie die in der nachfolgenden Tabelle beschriebenen Einstellungen anpassen.

Einstellungen der Regeln für Netzwerkpakete

Einstellung	Beschreibung
Name	Name der Netzwerkpaketregel
Aktion	Aktion, welche die Komponente "Firewall-Verwaltung" bei Erkennen von Netzwerkaktivität ausführt.
Lokale Adresse	Netzwerkadressen der Geräte, auf denen die App Kaspersky Endpoint Security installiert ist und die Netzwerkpakete senden und empfangen können
Remote-Adresse	Netzwerkadressen der Remote-Geräte, die Netzwerkpakete senden und/oder empfangen können.
Richtung	Richtung der überwachten Netzwerkaktivität.
Protokoll	Typ des Datenübertragungsprotokolls, für den die Netzwerkaktivität überwacht werden soll.
Lokale Ports	Portnummern von lokalen Geräten, zwischen denen die Verbindung überwacht wird.
Remote-Ports	Portnummern von Remote-Geräten, zwischen denen die Verbindung überwacht wird.
ICMP-Typ	ICMP-Typ. Die Komponente zur Firewall-Verwaltung überwacht Nachrichten des angegebenen Typs, die vom Host oder vom Gateway gesendet werden.
ICMP-Code	ICMP-Code. Die Firewall-Verwaltung überwacht Nachrichten des im Feld **ICMP-Typ** angegebenen Typs mit dem im Feld **ICMP-Code** angegebenen Code, die vom Host oder Gateway gesendet werden.
Protokollierung	Diese Spalte gibt an, ob die App die Aktionen der Netzwerkpaketregel protokolliert. Wenn in der Spalte **Ja** angegeben ist, protokolliert die App die Aktionen der Netzwerkpaketregel. Wenn in der Spalte **Nein** angegeben ist, protokolliert die App die Aktionen der Netzwerkpaketregel nicht.

Standardmäßig ist die Tabelle mit Regeln für Netzwerkpakete leer.

Sie können Netzwerkpaketregeln in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.

Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Regel für Netzwerkpakete"

In diesem Fenster können Sie die Regel für Netzwerkpakete anpassen.

Einstellungen der Netzwerkpaketregel

Einstellung	Beschreibung
Regelname	Eingabefeld für den Namen der Netzwerkpaketregel.
Aktion	In der Dropdown-Liste können Sie eine Aktion festlegen, welche die Komponente "Firewall-Verwaltung" ausführen soll, sobald sie die Netzwerkaktivität erkennt: • Netzwerkaktivität **blockieren**. • Netzwerkaktivität **erlauben** (Standardwert).
Protokoll	In der Dropdown-Liste können Sie den Typ des Datenübertragungsprotokolls wählen, für das die Netzwerkaktivität überwacht werden soll: • **Beliebig** (Standardwert) • **GRE** • **ICMP** • **ICMPv6** • **IGMP** • **TCP** • **UDP**
Geben Sie den ICMP-Typ an	Mithilfe dieses Kontrollkästchens können Sie den geben Sie den ICMP-Typ an. Die Komponente "Firewall-Verwaltung" überwacht dann Nachrichten des angegebenen Typs, die vom Host oder vom Gateway gesendet werden.

	Wenn dieses Kontrollkästchen aktiviert ist, wird ein Eingabefeld für den ICMP-Typ angezeigt. Dieses Kontrollkästchen wird nur angezeigt, wenn als Datenübertragungsprotokoll in der Dropdown-Liste **Protokoll** die Option **ICMP** oder **ICMPv6** ausgewählt wurde. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Geben Sie den ICMP-Code an	Mithilfe dieses Kontrollkästchens können Sie den geben Sie den ICMP-Code an. Die Firewall-Verwaltung überwacht Nachrichten des angegeben Typs (im Feld unterhalb des Kontrollkästchens **ICMP-Typ angeben**) mit dem angegebenen Code (im Feld unterhalb des Kontrollkästchens **ICMP-Code angeben**), die vom Host oder Gateway gesendet werden. Wenn dieses Kontrollkästchen aktiviert ist, wird ein Eingabefeld für den ICMP-Code angezeigt. Dieses Kontrollkästchen wird nur angezeigt, wenn als Datenübertragungsprotokoll in der Dropdown-Liste **Protokoll** die Option **ICMP** oder **ICMPv6** ausgewählt wurde und das Kontrollkästchen **Geben Sie den ICMP-Typ an** aktiviert ist. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Richtung	In dieser Dropdown-Liste können Sie die Richtung der zu überwachenden Netzwerkaktivität festlegen: • **Eingehende Pakete** (Standardwert). Wenn dieses Element ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" eingehende Pakete. • **Eingehend**. Wenn dieses Element ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" eingehende Netzwerkaktivitäten. • **Eingehend/Ausgehend**. Wenn dieses Element ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" sowohl eingehende als auch ausgehende Netzwerkaktivitäten. • **Eingehende/Ausgehende Pakete**. Wenn dieses Element ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" sowohl eingehende als auch ausgehende Pakete. • **Ausgehende Pakete**. Wenn dieses Element ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" ausgehende Pakete. • **Ausgehend**. Wenn dieses Element ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" ausgehende Netzwerkaktivitäten.
Remote-Adresse	In dieser Dropdown-Liste können Sie die Netzwerkadressen der Remote-Geräte angeben, die Netzwerkpakete senden und empfangen können: • **Beliebige Adresse** (Standardwert). Wenn dieses Element ausgewählt ist, kontrolliert die Netzwerkregel Netzwerkpakete, die von Remote-Computern mit jeder IP-Adresse gesendet bzw. empfangen werden. • **Alle Subnetzadressen**. Wenn dieses Element ausgewählt ist, kontrolliert die Netzwerkregel Netzwerkpakete, die von bestimmten Remote-Geräten gesendet und empfangen werden. Die IP-Adressen dieser Remote-Computer gehören in diesem Fall zu dem weiter unten ausgewählten Netzwerktyp: **Öffentliche Netzwerke**, **Lokale Netzwerke** oder **Vertrauenswürdige Netzwerke**. • **Angegebene Adresse**. Wenn dieses Element ausgewählt ist, kontrolliert die Netzwerkregel Netzwerkpakete, die von Remote-Geräten mit IP-Adressen gesendet und/oder empfangen wurden, die im Eingabefeld **Adresse** angegeben sind.
Geben Sie die	Mithilfe dieses Kontrollkästchens können Sie die Portnummern der Remote-Geräten

Remote-Ports an	angeben, zwischen denen die Verbindungen überwacht werden sollen. Wenn dieses Kontrollkästchen aktiviert ist, wird ein Eingabefeld für den Port angezeigt. Dieses Kontrollkästchen wird nur angezeigt, wenn als Datenübertragungsprotokoll in der Dropdown-Liste **Protokoll** die Option **TCP** oder **UDP** ausgewählt wurde. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Lokale Adresse	In dieser Dropdown-Liste können Sie die Netzwerkadressen der Geräte angeben, auf denen die App Kaspersky Endpoint Security installiert ist und die Netzwerkpakete senden bzw. empfangen können: • **Beliebige Adresse** (Standardwert). Wenn dieses Element ausgewählt ist, kontrolliert die Netzwerkregel Netzwerkpakete, die von Geräten mit installierter App Kaspersky Endpoint Security und beliebigen IP-Adressen gesendet und empfangen werden. • **Angegebene Adresse**. Wenn dieses Element ausgewählt ist, kontrolliert die Netzwerkregel die im Feld **Adresse** angegebenen Netzwerkadressen der Geräte auf denen die App Kaspersky Endpoint Security installiert ist und die Netzwerkpakete senden und empfangen können.
Geben Sie die lokalen Ports an	Mithilfe dieses Kontrollkästchens können Sie die Portnummern der Remote-Geräte angeben, zwischen denen die Verbindungen überwacht werden sollen. Wenn dieses Kontrollkästchen aktiviert ist, wird ein Eingabefeld für den Port angezeigt. Dieses Kontrollkästchen wird nur angezeigt, wenn als Datenübertragungsprotokoll in der Dropdown-Liste **Protokoll** die Option **TCP** oder **UDP** ausgewählt wurde. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Protokollieren	Mithilfe dieses Kontrollkästchens können Sie angeben, ob die Aktionen der Regel für Netzwerkpakete im Bericht protokolliert werden sollen. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App die Aktionen der Netzwerkregel. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die App die Aktionen der Netzwerkregel nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Fenster "Verfügbare Netzwerke"

Die Tabelle **Verfügbare Netzwerke** enthält Netzwerke, die von der Komponente "Firewall-Verwaltung" überwacht werden. Standardmäßig ist die Tabelle mit verfügbaren Netzwerken leer.

Einstellungen für verfügbare Netzwerke

Einstellung	Beschreibung
IP-Adresse	Netzwerk-IP-Adresse.
Netzwerktyp	Netzwerktyp (**Öffentliches Netzwerk**, **Lokales Netzwerk** oder **Vertrauenswürdiges Netzwerk**).

Sie können verfügbare Netzwerke hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Netzwerkverbindung"

In diesem Fenster können Sie eine Netzwerkverbindung anpassen, die von der Komponente "Firewall-Verwaltung" überwacht werden soll.

Netzwerkverbindung

Einstellung	Beschreibung
IP-Adresse	Eingabefeld für die Netzwerk-IP-Adresse.
Netzwerktyp	Sie können den Netzwerktyp wählen: • **Öffentliches Netzwerk** • **Lokales Netzwerk** • **Vertrauenswürdiges Netzwerk**

Firewall-Verwaltung in der Verwaltungskonsole

In der Verwaltungskonsole können Sie Einstellungen der Firewall-Verwaltung in den Einstellungen der Richtlinie konfigurieren (**Basisschutz** → **Firewall-Verwaltung**).

Einstellungen der Komponente "Firewall-Verwaltung"

Einstellung	Beschreibung
Firewall-Verwaltung aktivieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Komponente "Firewall-Verwaltung". Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Netzwerkpaketregeln	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Netzwerkpaketregeln** öffnet. In diesem Fenster können Sie die Netzwerkpaketregeln konfigurieren, die von der Komponente "Firewall-Verwaltung" angewendet werden, wenn eine versuchte Netzwerkverbindung erkannt wird.
Verfügbare Netzwerke	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Verfügbare Netzwerke** öffnet. In diesem Fenster können Sie eine Liste mit Netzwerken festlegen, die von der Komponente "Firewall-Verwaltung" überwacht werden sollen.
Eingehende Verbindungen	In dieser Dropdown-Liste können Sie eine Aktion auswählen, die für eingehende Netzwerkverbindungen ausgeführt wird: • Netzwerkverbindungen **erlauben** (Standardwert).

	• Eingehende Netzwerkverbindungen **blockieren**.
Eingehende Pakete	In dieser Dropdown-Liste können Sie eine Aktion auswählen, die für eingehende Pakete ausgeführt wird: • Eingehende Pakete **erlauben** (Standardwert). • Eingehende Pakete **blockieren**.
Erlaubnisregeln für Ports des Administrationsagenten immer hinzufügen	Dieses Kontrollkästchen aktiviert oder deaktiviert das automatische Hinzufügen von Erlaubnisregeln für Ports des Administrationsagent. Das Kontrollkästchen ist standardmäßig aktiviert.

Fenster "Regeln für Netzwerkpakete"

Die Tabelle **Netzwerkpaketregeln** enthält Regeln für Netzwerkpakete, die von der Komponente "Firewall-Verwaltung" zur Überwachung der Netzwerkaktivität verwendet werden. Für Netzwerkpaketregeln können Sie die in der nachfolgenden Tabelle beschriebenen Einstellungen anpassen.

Einstellungen der Regeln für Netzwerkpakete

Einstellung	Beschreibung
Name	Name der Netzwerkpaketregel
Aktion	Aktion, welche die Komponente "Firewall-Verwaltung" bei Erkennen von Netzwerkaktivität ausführt.
Lokale Adresse	Netzwerkadressen der Geräte, auf denen die App Kaspersky Endpoint Security installiert ist und die Netzwerkpakete senden und empfangen können
Remote-Adresse	Netzwerkadressen der Remote-Geräte, die Netzwerkpakete senden und/oder empfangen können.
Protokollierung	Diese Spalte gibt an, ob die App die Aktionen der Netzwerkpaketregel protokolliert. Wenn in der Spalte **Ja** angegeben ist, protokolliert die App die Aktionen der Netzwerkpaketregel. Wenn in der Spalte **Nein** angegeben ist, protokolliert die App die Aktionen der Netzwerkpaketregel nicht.

Standardmäßig ist die Tabelle mit Regeln für Netzwerkpakete leer.

Sie können Netzwerkpaketregeln in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.

Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Netzwerkpaketregel hinzufügen"

In diesem Fenster können Sie die Einstellungen der hinzuzufügenden Netzwerkpaketregel anpassen.

Einstellungen der Netzwerkpaketregel

Einstellung	Beschreibung
Protokoll	Sie können den Typ des Datenübertragungsprotokolls wählen, für das die Netzwerkaktivität überwacht werden soll: • **Beliebig** (Standardwert) • **GRE** • **ICMP** • **ICMPv6** • **IGMP** • **TCP** • **UDP**
Richtung	Sie können die Richtung der zu überwachenden Netzwerkaktivität festlegen: • **Eingehende Pakete**. Wenn diese Option ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" eingehende Pakete. • **Eingehend**. Wenn diese Option ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" eingehende Netzwerkaktivitäten. • **Eingehend/Ausgehend**. Wenn diese Option ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" sowohl eingehende als auch ausgehende Netzwerkaktivitäten. • **Eingehende/Ausgehende Pakete**. Wenn diese Option ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" sowohl eingehende als auch ausgehende Pakete. • **Ausgehende Pakete**. Wenn diese Option ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" ausgehende Pakete.

	• **Ausgehend**. Wenn diese Option ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" ausgehende Netzwerkaktivitäten.
ICMP-Typ	Sie können den geben Sie den ICMP-Typ an. Die Komponente "Firewall-Verwaltung" überwacht dann Nachrichten des angegebenen Typs, die vom Host oder vom Gateway gesendet werden. Wenn die Option **Angegeben** ausgewählt wurde, wird ein Eingabefeld für den ICMP-Typ angezeigt. Dieses Fenster wird angezeigt, wenn als Datenübertragungsprotokoll in der Dropdown-Liste **Protokoll** die Option **ICMP** oder **ICMPv6** ausgewählt wurde.
ICMP-Code	Sie können den geben Sie den ICMP-Code an. Die Firewall-Verwaltung überwacht Nachrichten des im Feld **ICMP-Typ** angegebenen Typs mit dem im Feld **ICMP-Code** angegebenen Code, die vom Host oder Gateway gesendet werden. Wenn die Option **Angegeben** ausgewählt wurde, wird ein Eingabefeld für den ICMP-Code angezeigt. Dieses Fenster wird angezeigt, wenn als Datenübertragungsprotokoll in der Dropdown-Liste **Protokoll** die Option **ICMP** oder **ICMPv6** ausgewählt wurde.
Remote-Ports	Sie können die Portnummern der Remote-Geräte angeben, zwischen denen die Verbindungen überwacht werden sollen. Wenn die Option **Angegeben** ausgewählt wurde, wird ein Eingabefeld für die Portnummern angezeigt. Dieses Fenster wird angezeigt, wenn als Datenübertragungsprotokoll in der Dropdown-Liste **Protokoll** die Option **TCP** oder **UDP** ausgewählt wurde.
Lokale Ports	Sie können die Portnummern der lokalen Geräte angeben, zwischen denen die Verbindungen überwacht werden sollen. Wenn die Option **Angegeben** ausgewählt wurde, wird ein Eingabefeld für die Portnummern angezeigt. Dieses Fenster wird angezeigt, wenn als Datenübertragungsprotokoll in der Dropdown-Liste **Protokoll** die Option **TCP** oder **UDP** ausgewählt wurde.
Remote-Adressen	Sie können die Netzwerkadressen der Remote-Geräte angeben, die Netzwerkpakete senden und empfangen können: • **Beliebige Adresse** (Standardwert). Wenn dieses Element ausgewählt ist, kontrolliert die Netzwerkregel Netzwerkpakete, die von Remote-Geräten mit jeder IP-Adresse gesendet bzw. empfangen werden. • **Angegebene Adresse**. Wenn diese Option ausgewählt ist, kontrolliert die Netzwerkregel Netzwerkpakete, die von Remote-Geräten mit den IP-Adressen, die im Eingabefeld darunter angegeben sind, gesendet und empfangen wurden. • **Nach Netzwerktyp**. Wenn diese Option ausgewählt ist, kontrolliert die Netzwerkregel Netzwerkpakete, die von bestimmten Remote-Geräten gesendet und empfangen werden. Die IP-Adressen dieser Remote-Geräte gehören in diesem Fall zu dem weiter unten ausgewählten Netzwerktyp: **Öffentliche Netzwerke**, **Lokale Netzwerke** oder **Vertrauenswürdige Netzwerke**.
Lokale Adressen	Sie können die Netzwerkadressen der Geräte angeben, auf denen die App Kaspersky Endpoint Security installiert ist und die Netzwerkpakete senden und empfangen können: • **Beliebige Adresse** (Standardwert). Wenn dieses Option ausgewählt ist, kontrolliert die Netzwerkregel Netzwerkpakete, die von Geräten mit installierter App Kaspersky Endpoint Security und beliebigen IP-Adressen gesendet und empfangen werden.

	• **Angegebene Adresse**. Wenn diese Option ausgewählt ist, kontrolliert die Netzwerkregel die im Feld darunter angegebenen Netzwerkadressen der Geräte auf denen die App Kaspersky Endpoint Security installiert ist und die Netzwerkpakete senden und empfangen können.
Aktion	Sie können eine Aktion festlegen, welche die Komponente "Firewall-Verwaltung" ausführen soll, sobald sie die Netzwerkaktivität erkennt: • Netzwerkaktivität **blockieren**. • Netzwerkaktivität **erlauben** (Standardwert).
Protokollierung	Sie können angeben, ob die Aktionen der Netzwerkregel im Bericht protokolliert werden sollen.
Regelname	Eingabefeld für den Namen der Netzwerkpaketregel.

Fenster "Verfügbare Netzwerke"

Die Tabelle **Verfügbare Netzwerke** enthält Netzwerke, die von der Komponente "Firewall-Verwaltung" überwacht werden. Standardmäßig ist die Tabelle mit verfügbaren Netzwerken leer.

Einstellungen für verfügbare Netzwerke

Einstellung	Beschreibung
IP-Adresse	Netzwerk-IP-Adresse.
Netzwerktyp	Netzwerktyp (**Öffentliches Netzwerk**, **Lokales Netzwerk** oder **Vertrauenswürdiges Netzwerk**).

Sie können verfügbare Netzwerke hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Netzwerkverbindung"

In diesem Fenster können Sie eine Netzwerkverbindung anpassen, die von der Komponente "Firewall-Verwaltung" überwacht werden soll.

Netzwerkverbindung

Einstellung	Beschreibung

IP-Adresse	Eingabefeld für die Netzwerk-IP-Adresse.
Netzwerktyp	Sie können den Netzwerktyp wählen: • **Öffentliches Netzwerk** • **Lokales Netzwerk** • **Vertrauenswürdiges Netzwerk**

Firewall-Verwaltung über die Befehlszeile

Über die Befehlszeile können Sie die Firewall-Verwaltung mithilfe der vordefinierten Aufgabe "Firewall-Verwaltung" (*Firewall_Management*) konfigurieren.

Standardmäßig wird die Aufgabe "Firewall-Verwaltung" nicht gestartet. Sie können diese Aufgabe manuell starten und beenden.

Sie können die Einstellungen zur Firewall-Verwaltung konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe mithilfe des Befehls zur Verwaltung der Aufgabeneinstellungen ändern.

Sie können die Einstellungen zur Firewall-Verwaltung auch mithilfe der Befehle zur Firewall-Verwaltung konfigurieren:

- Erstellen und löschen Sie Netzwerkpaketregeln und ändern Sie ihre Ausführungspriorität.
- Erstellen Sie eine Liste von IP-Adressen oder Subnetzen in Netzwerkzonen.
- Zeigen Sie die in Kaspersky Endpoint Security erstellten Firewall-Regeln mit dem Befehl `kesl-control -F --query` an.

Einstellungen der Aufgabe zur Firewall-Verwaltung

Einstellung	Beschreibung	Werte
`DefaultIncomingAction`	Standardaktion, die mit einer eingehenden Verbindung ausgeführt werden soll, wenn für diese Verbindungsart keine Netzwerkregeln übernommen werden können.	`Allow` (Standardwert) – Eingehende Verbindungen zulassen. `Block` –Eingehende Verbindung blockieren.
`DefaultIncomingPacketAction`	Standardaktion, die mit einem eingehenden Paket ausgeführt werden soll, wenn für diese Verbindungsart keine Netzwerkpaketregeln übernommen werden können.	`Allow` (Standardwert) – Eingehende Pakete zulassen. `Block` – Eingehendes Paket blockieren.
`OpenNagentPorts`	Hinzufügen dynamischer Regeln für den Administrationsagenten zu den Paketregeln.	`Yes` (Standardwert) – Dynamische Regeln für den Netzwerkagenten zu den Paketregeln hinzufügen.

		`No` – Keine dynamischen Regeln für den Netzwerkagenten zu den Paketregeln hinzufügen.
Der Abschnitt **[PacketRules.item_#]** enthält Netzwerkpaketregeln für die Aufgabe zur Firewall-Verwaltung. Sie können mehrere Abschnitte `[PacketRules.item_#]` in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge. Jeder Abschnitt `[PacketRules.item_#]` enthält die folgenden Einstellungen:		
`Name`	Name der Netzwerkpaketregel.	Standardwert: `Packet rule #<n>`, wobei n ein Index ist.
`FirewallAction`	Aktion, die mit den in dieser Netzwerkpaketregel angegebenen Verbindungen ausgeführt wird.	`Allow` (Standardwert) – Netzwerkverbindungen zulassen. `Block` – Netzwerkverbindung blockieren.

`Protocol`	Typ des Protokolls, für das die Netzwerkaktivität überwacht werden soll.	`Any` (Standardwert) – Die Aufgabe zur Firewall-Verwaltung überwacht die gesamte Netzwerkaktivität.
		`TCP`
		`UDP`
		`ICMP`
		`ICMPv6`
		`IGMP`
		`GRE`

`RemotePorts`	Portnummern der Remote-Geräte, zwischen denen die Verbindungen überwacht werden sollen. Sie können den Wert als Ganzzahl oder als Intervall angeben. Diese Einstellung kann nur angegeben werden, wenn der Wert der Einstellung `Protocol` auf `TCP` oder `UDP` festgelegt wurde.	`Any` (Standardwert) – Alle Remote-Ports überwachen. `0` – `65535`
`LocalPorts`	Portnummern der lokalen Geräte, zwischen denen die Verbindungen überwacht werden sollen. Sie können den Wert als Ganzzahl oder als Intervall angeben. Diese Einstellung kann nur angegeben werden, wenn der Wert der Einstellung `Protocol` auf `TCP` oder `UDP` festgelegt wurde.	`Any` (Standardwert) – Alle lokalen Ports überwachen. `0` – `65535`.
`ICMPType`	ICMP-Pakettyp. Diese Einstellung kann nur angegeben werden, wenn der Wert der Einstellung `Protocol` auf `ICMP` oder `ICMPv6` festgelegt wurde.	`Any` (Standardwert) – Alle ICMP-Pakettypen überwachen. Ganzzahl entsprechend der Spezifikation eines Datentransferprotokolls

`ICMPCode`	ICMP-Paketcode. Diese Einstellung kann nur angegeben werden, wenn der Wert der Einstellung `Protocol` auf `ICMP` oder `ICMPv6` festgelegt wurde.	`Any` (Standardwert) – Alle Codes von ICMP-Paketen überwachen. Ganzzahl entsprechend der Spezifikation eines Datentransferprotokolls
`Direction`	Richtung der überwachten Netzwerkaktivität.	`IncomingOutgoing` oder `InOut` (Standardwert) – sowohl eingehende als auch ausgehende Verbindungen überwachen. `Incoming` oder `In` – Eingehende Verbindungen überwachen. `Outgoing` oder `Out` – Ausgehende Verbindungen überwachen. `IncomingPacket` oder `InPacket` – Eingehende Pakete überwachen. `OutgoingPacket` oder `OutPacket` – Ausgehende Pakete überwachen. `IncomingOutgoingPacket` oder `InOutPacket` – sowohl eingehende als auch ausgehende Pakete überwachen.
`RemoteAddress`	Netzwerkadressen der Remote-Geräte, die Netzwerkpakete senden und empfangen können.	`Any` (Standardwert) – Netzwerkpakete überwachen, die von Remote-Geräten mit beliebiger IP-Adresse gesendet und/oder empfangen wurden. `Trusted` – Vordefinierte Netzwerkzone für vertrauenswürdige Netzwerke. `Local` – Vordefinierte Netzwerkzone für lokale Netzwerke. `Public` – Vordefinierte Netzwerkzone für öffentliche Netzwerke. `d.d.d.d` – IPv4-Adresse, wobei d eine Dezimalzahl von 0 bis 255 ist. `d.d.d.d/p` – Subnetz von IPv4-Adressen, wobei p eine Zahl von 0 bis 32 ist.

		`x:x:x:x:x:x:x:x` – IPv6-Adresse, wobei x eine hexadezimale Zahl von 0 bis ffff ist. `x:x:x:x::0/p` – Subnetz von IPv6-Adressen, wobei p eine Zahl von 0 bis 64 ist.
`LocalAddress`	Netzwerkadressen der Geräte, auf denen die App Kaspersky Endpoint Security installiert ist und die Netzwerkpakete senden und empfangen können	`Any` (Standardwert) – Netzwerkpakete überwachen, die von lokalen Geräten mit beliebiger IP-Adresse gesendet und/oder empfangen wurden. `d.d.d.d` – IPv4-Adresse, wobei d eine Dezimalzahl von 0 bis 255 ist. `d.d.d.d/p` – Subnetz von IPv4-Adressen, wobei p eine Zahl von 0 bis 32 ist. `x:x:x:x:x:x:x:x` – IPv6-Adresse, wobei x eine hexadezimale Zahl von 0 bis ffff ist. `x:x:x:x::0/p` – Subnetz von IPv6-Adressen, wobei p eine Zahl von 0 bis 64 ist.
`LogAttempts`	Aktiviert das Protokollieren von Aktionen der Netzwerkregel im Bericht.	`Yes` – Aktionen im Bericht protokollieren. `No` (Standardwert) – Aktionen nicht im Bericht protokollieren.
Der Abschnitt **[NetworkZonesPublic]** enthält die Netzwerkadressen, die mit öffentlichen Netzwerken assoziiert sind. Sie können mehrere IP-Adressen oder Subnetze von IP-Adressen angeben.		
`Address.item_#`	Gibt die IP-Adresse oder das IP-Subnetz an.	`d.d.d.d` – IPv4-Adresse, wobei d eine Dezimalzahl von 0 bis 255 ist. `d.d.d.d/p` – Subnetz von IPv4-Adressen, wobei p eine Zahl von 0 bis 32 ist. `x:x:x:x:x:x:x:x` – IPv6-Adresse, wobei x eine hexadezimale Zahl von 0 bis ffff ist. `x:x:x:x::0/p` – Subnetz von IPv6-Adressen, wobei p eine Zahl von 0 bis 64 ist. Standardwert: "" (keine Netzwerkadressen in dieser Zone).
Der Abschnitt **[NetworkZonesLocal]** enthält Netzwerkadressen, die mit lokalen Netzwerken assoziiert sind. Sie können mehrere IP-Adressen oder Subnetze von IP-Adressen angeben.		

`Address.item_#`	Gibt die IP-Adresse oder das IP-Subnetz an.	`d.d.d.d` – IPv4-Adresse, wobei d eine Dezimalzahl von 0 bis 255 ist. `d.d.d.d/p` – Subnetz von IPv4-Adressen, wobei p eine Zahl von 0 bis 32 ist. `x:x:x:x:x:x:x:x` – IPv6-Adresse, wobei x eine hexadezimale Zahl von 0 bis ffff ist. `x:x:x:x::0/p` – Subnetz von IPv6-Adressen, wobei p eine Zahl von 0 bis 64 ist. Standardwert: `""` (keine Netzwerkadressen in dieser Zone).
Der Abschnitt **[NetworkZonesTrusted]** enthält Netzwerkadressen, die mit vertrauenswürdigen Netzwerken assoziiert sind. Sie können mehrere IP-Adressen oder Subnetze von IP-Adressen angeben.		
`Address.item_#`	Gibt die IP-Adresse oder das IP-Subnetz an.	`d.d.d.d` – IPv4-Adresse, wobei d eine Dezimalzahl von 0 bis 255 ist. `d.d.d.d/p` – Subnetz von IPv4-Adressen, wobei p eine Zahl von 0 bis 32 ist. `x:x:x:x:x:x:x:x` – IPv6-Adresse, wobei x eine hexadezimale Zahl von 0 bis ffff ist. `x:x:x:x::0/p` – Subnetz von IPv6-Adressen, wobei p eine Zahl von 0 bis 64 ist. Standardwert: `""` (keine Netzwerkadressen in dieser Zone).

Liste der Netzwerkpaketregeln über die Befehlszeile konfigurieren

Um eine Netzwerkpaketregel hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --add-rule [--name <Regelname>] [--action <Aktion>] [--protocol
<Protokoll>] [--direction <Richtung>] [--remote <Remote-Adresse>[:<Portbereich>]] [--
local <lokale Adresse>[:<Portbereich>]] [--at <Index>]
```

Wobei gilt:

- `--name <Regelname>` – Name der Netzwerkpaketregel.
- `--action <Aktion>` – Aktion, die mit den in dieser Netzwerkpaketregel angegebenen Verbindungen ausgeführt wird.

- `--protocol <Protokoll>` – Typ des Datenübertragungsprotokolls, für das Sie die Netzwerkaktivität überwachen wollen.
- `--direction <Richtung>` – Richtung der überwachten Netzwerkaktivität.
- `--remote <Remote-Adresse[:<Portbereich>]>` – Netzwerkadresse des Remote-Geräts. Als Remote-Adresse können Sie den Namen einer vordefinierten Netzwerkzone angeben.
- `--local <lokale Adresse[:<Portbereich>]>` – Netzwerkadresse des Geräts, auf dem Kaspersky Endpoint Security installiert ist.
- `--at <Index>` – Index der Regel in der Liste der Netzwerkpaketregeln. Wenn der Schalter `--at` nicht angegeben wird oder sein Wert größer als die Anzahl der Regeln in der Liste ist, wird die neue Regel zum Ende der Liste hinzugefügt.

Einstellungen, für die Sie im Befehl keine Werte angeben, werden auf ihre Standardwerte gesetzt.

Beispiele:
Führen Sie den folgenden Befehl aus, um eine Regel zu erstellen, die alle eingehenden und hergestellten Verbindungen zum TCP-Port 23 blockiert:
```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote any
```
Führen Sie den folgenden Befehl aus, um eine Regel zu erstellen, die eingehende und hergestellte Verbindungen zum TCP-Port 23 für die Öffentliche Netzwerkzone blockiert:
```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote Public
```

Um eine Netzwerkpaketregel zu löschen, führen Sie einen der folgenden Befehle aus:

- `kesl-control --del-rule --name <Regelname>`
- `kesl-control --del-rule --index <Index>`

  Wobei gilt:

- `--name <Regelname>` – Name der Netzwerkpaketregel.
- `--index <Index>` – Aktueller Index der Regel in der Liste der Netzwerkpaketregeln.

Wenn die Netzwerkpaketregelliste mehrere Regeln mit demselben Namen oder keine Regel mit dem angegebenen Namen oder Index enthält, tritt ein Fehler auf.

Um eine Ausführungspriorität für eine Netzwerkpaketregel zu ändern, führen Sie einen der folgenden Befehle aus:

- `kesl-control --move-rule --name <Regelname> --at <Index>`
- `kesl-control --move-rule --index <Index> --at <Index>`

  Wobei gilt:

- `--name <Regelname>` – Name der Netzwerkpaketregel.
- `--index <Index>` – Aktueller Index der Regel in der Liste der Netzwerkpaketregeln.
- `--at <Index>` – Neuer Regelindex in der Liste der Netzwerkpaketregeln.

Netzwerkzonen über die Befehlszeile konfigurieren

Um eine Netzwerkadresse zur Zone hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --add-zone --zone <Zone> --address <Adresse>
```

Wobei gilt:

- `--zone <Zone>` – Vordefinierter Name der Netzwerkzone. Mögliche Werte: `Public`, `Local`, `Trusted`.
- `--address <Adresse>` – Netzwerkadresse oder Subnetz.

Um eine Netzwerkadresse aus der Zone zu löschen, führen Sie einen der folgenden Befehle aus:

- `kesl-control --del-zone --zone <Zone> --address <Adresse>`
- `kesl-control --del-zone --zone <Zone> --index <Adressindex in der Zone>`

Wenn eine Zone mehrere Elemente mit derselben Netzwerkadresse enthält, wird der Befehl `--del-zone` nicht ausgeführt.

Wenn die angegebene Netzwerkadresse oder der Index nicht existiert, wird eine Fehlermeldung angezeigt.

Schutz vor Web-Bedrohungen

Mit der Komponente "Schutz vor Web-Bedrohungen" können Sie eingehenden Datenverkehr, der über HTTP-, HTTPS- und FTP-Protokolle übertragen wird, Websites und IP-Adressen untersuchen, das Herunterladen schädlicher Dateien aus dem Internet verhindern und den Zugriff auf Phishing-, Adware- und andere gefährliche Websites blockieren.

Diese Funktionalität wird im KESL-Container nicht unterstützt.

Aktuelle Verbindungen für abgefangene TCP-Ports werden zurückgesetzt, wenn der Schutz vor Netzwerkbedrohungen aktiviert ist.

Standardmäßig ist der Schutz vor Web-Bedrohungen deaktiviert. Er wird jedoch automatisch aktiviert, wenn die lokale Verwaltung der Einstellungen für den Schutz vor Web-Bedrohungen auf dem Gerät erlaubt ist (die Richtlinie wird nicht angewendet oder das "Schloss" ist in den Eigenschaften der Richtlinie nicht gesetzt) und wenn eine der folgenden ausführbaren Browserdateien, einschließlich im Snap-Format, im System erkannt wird:

- chrome
- chromium
- chromium-browser
- firefox
- firefox-esr
- google-chrome
- opera
- yandex-browser

Sie können den Schutz vor Web-Bedrohungen ein- und ausschalten und auch Schutzeinstellungen konfigurieren:

- Wählen Sie eine Aktion aus, die von der App auf eine Webressource angewendet werden soll, auf der ein gefährliches Objekt erkannt wird.
- Konfigurieren Sie eine Liste mit vertrauenswürdigen Webadressen. Die App untersucht nicht den Inhalt von Websites, deren Webadressen in dieser Liste aufgeführt sind.
- Wählen Sie Objekte aus, die die App während der Untersuchung des eingehenden Datenverkehrs erkennen soll.
- Konfigurieren Sie die Untersuchung geschützter Verbindungen, um den HTTPS-Verkehr zu untersuchen.

  Um den FTP-Verkehr zu untersuchen, muss in den Einstellungen zur Untersuchung geschützter Verbindungen die Kontrolle aller Netzwerkports konfiguriert werden.

Beim Öffnen einer Website führt die App folgende Aktionen aus:

1. Sie überprüft die Sicherheit der Website mithilfe der heruntergeladenen App-Datenbanken.
2. Sie überprüft die Sicherheit der Website mithilfe der heuristischen Analyse, sofern diese aktiviert ist.

Während der heuristischen Analyse analysiert Kaspersky Endpoint Security die Aktivität von Anwendungen im Betriebssystem. Die heuristische Analyse kann gefährliche Objekte erkennen, für die derzeit keine Einträge in den Datenbanken von Kaspersky Endpoint Security vorliegen.

3. Wenn die Verwendung von Kaspersky Security Network aktiviert ist, wird die Zuverlässigkeit einer Website anhand der Reputationsdatenbanken von Kaspersky geprüft.

   Es wird empfohlen, die Verwendung von Kaspersky Security Network zu aktivieren, um die Wirksamkeit des Schutzes vor Web-Bedrohungen zu steigern.

4. Sie blockiert bzw. erlaubt das Öffnen der Website.

Beim Versuch, eine gefährliche Website zu öffnen, führt die App folgende Aktionen aus:

- Für HTTP- oder FTP-Verkehr blockiert die App den Zugriff und zeigt eine Warnung an.
- Für HTTPS-Verkehr zeigt der Browser eine Fehlerseite an.

Das Entfernen von App-Zertifikaten kann zu einer fehlerhaften Ausführung der Komponente "Schutz vor Web-Bedrohungen" führen.

Kaspersky Endpoint Security fügt zur Liste der Tabelle mangle der Tools iptables und ip6tables eine spezielle Erlaubniskette der Regeln kesl_bypass hinzu, die es erlaubt, den Datenverkehr von der Untersuchung durch die App auszuschließen. Wenn in der Kette Ausschlussregeln für den Datenverkehr konfiguriert sind, wirken sie sich auf die Ausführung der Komponente "Schutz vor Web-Bedrohungen" aus.

Schutz vor Web-Bedrohungen in der Web Console konfigurieren

In der Web Console können Sie Einstellungen des Schutzes vor Web-Bedrohungen in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen** → **Basisschutz** → **Schutz vor Web-Bedrohungen**).

Einstellungen der Komponente "Schutz vor Web-Bedrohungen"

Einstellung	Beschreibung
Schutz vor Web-Bedrohungen aktiviert/deaktiviert	Der Schalter aktiviert bzw. deaktiviert die Komponente "Schutz vor Web-Bedrohungen". Der Schalter ist standardmäßig deaktiviert.
Aktion beim Erkennen einer Bedrohung	In diesem Abschnitt können Sie eine Aktion angeben, die von der App für Webressourcen ausgeführt werden soll, in denen ein gefährliches Objekt gefunden wird: • Benutzer **informieren**, wenn im Web-Datenverkehr ein gefährliches Objekt erkannt wird. Der Schutz vor Web-Bedrohungen erlaubt den Download dieses Objekts auf das Gerät. Dabei protokolliert die App Informationen über das gefährliche Objekt und fügt Informationen über das gefährliche Objekt zur Liste der aktiven Bedrohungen hinzu. • Den Zugriff auf gefährliche Objekte, die im Web-Datenverkehr erkannt wurden, **blockieren**, eine Benachrichtigung über den blockierten Zugriffsversuch

	anzeigen und Informationen über das gefährliche Objekt im Protokoll speichern (Standardwert).
Schädliche Objekte erkennen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Überprüfung von Links gegen Datenbanken mit bösartigen Webadressen. Das Kontrollkästchen ist standardmäßig aktiviert.
Phishing-Links erkennen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Überprüfung von Links gegen Datenbanken mit Phishing-Adressen. Das Kontrollkästchen ist standardmäßig aktiviert.
Heuristische Analyse zum Erkennen von Phishing-Links verwenden	Dieses Kontrollkästchen aktiviert oder deaktiviert die Verwendung der heuristischen Analyse zur Erkennung von Phishing-Links. Dieses Kontrollkästchen ist verfügbar und standardmäßig aktiviert, wenn das Kontrollkästchen **Phishing-Links erkennen** aktiviert ist.
Adware erkennen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Überprüfung von Links gegen die Datenbanken von Adware-Webadressen. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Legale Programme erkennen, die von Angreifern zur Beschädigung von Geräten oder Daten ausgenutzt werden können	Dieses Kontrollkästchen aktiviert oder deaktiviert die Überprüfung von Links gegen die Datenbanken legitimer Anwendungen, mit denen Hacker Geräte oder Daten beschädigen können. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Vertrauenswürdige Webadressen	Diese Tabelle enthält Webadressen und Webseiten, deren Inhalt Sie vertrauen. Sie können nur HTTP-/HTTPS-Webadressen zur Liste der vertrauenswürdigen Webadressen hinzufügen. Für die Angabe der Webadressen können Sie Masken verwenden. IP-Adressen können nicht mit Masken beschrieben werden. Sie können beim Erstellen einer Adressmaske das Sternchen (*) als Platzhalter für ein oder mehrere Zeichen verwenden. Wenn Sie also die Adressmaske *abc* eingeben, wird sie auf alle Webressourcen angewendet, welche die Sequenz abc enthalten (z. B. www.virus.com/download_virus/page_0-9abcdef.html). Um das Sternchen als Zeichen und nicht als Maske in die Adressmaske aufzunehmen, geben Sie das Zeichen * zweimal ein (z. B. wird mit www.virus.com/**/page_0-9abcdef.html der Link www.virus.com/*/page_0-9abcdef.html dargestellt). Standardmäßig ist die Tabelle leer. Sie können die Webadressen in der Tabelle hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Webadresse"

In diesem Fenster können Sie Webadressen oder eine Maske für Webadressen hinzufügen, die Sie als vertrauenswürdig einstufen.

Sie können nur HTTP-/HTTPS-Webadressen zur Liste der vertrauenswürdigen Webadressen hinzufügen. Für die Angabe der Webadressen können Sie Masken verwenden. IP-Adressen können nicht mit Masken beschrieben werden.

Sie können beim Erstellen einer Adressmaske das Sternchen (*) als Platzhalter für ein oder mehrere Zeichen verwenden. Wenn Sie also die Adressmaske *abc* eingeben, wird sie auf alle Webressourcen angewendet, welche die Sequenz abc enthalten (z. B. www.virus.com/download_virus/page_0-9abcdef.html). Um das Sternchen als Zeichen und nicht als Maske in die Adressmaske aufzunehmen, geben Sie das Zeichen * zweimal ein (z. B. wird mit www.virus.com/**/page_0-9abcdef.html der Link www.virus.com/*/page_0- 9abcdef.html dargestellt).

Schutz vor Web-Bedrohungen in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie Einstellungen des Schutzes vor Web-Bedrohungen in den Richtlinieneigenschaften konfigurieren (**Allgemeine Einstellungen** → **Schutz vor Web-Bedrohungen**).

Einstellungen der Komponente "Schutz vor Web-Bedrohungen"

Einstellung	Beschreibung
Schutz vor Web-Bedrohungen aktivieren	Mit diesem Kontrollkästchen wird die Komponente "Schutz vor Web-Bedrohungen" aktiviert und deaktiviert. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Vertrauenswürdige Webadressen	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Vertrauenswürdige Webadressen** öffnet. In diesem Fenster können Sie eine Liste mit vertrauenswürdigen Webadressen angeben. Die App untersucht nicht den Inhalt von Websites, deren Webadressen in dieser Liste aufgeführt sind.
Aktion beim Erkennen einer Bedrohung	Aktion, die von der App auf eine Webressource angewendet wird, auf der ein gefährliches Objekt erkannt wird: • Den Zugriff auf gefährliche Objekte, die im Web-Datenverkehr erkannt wurden, **blockieren**, eine Benachrichtigung über den blockierten Zugriffsversuch anzeigen und Informationen über das gefährliche Objekt im Protokoll speichern (Standardwert). • Benutzer **informieren**, wenn im Web-Datenverkehr ein gefährliches Objekt erkannt wird. Der Schutz vor Web-Bedrohungen erlaubt den Download dieses Objekts auf das Gerät. Dabei protokolliert die App Informationen über das gefährliche Objekt und fügt Informationen über das gefährliche Objekt zur Liste der aktiven Bedrohungen hinzu.

Untersuchungseinstellungen	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Untersuchungseinstellungen** öffnet. In diesem Fenster können Sie die Einstellungen des eingehenden Datenverkehrs anpassen.

Fenster "Vertrauenswürdige Webadressen"

In diesem Fenster können Sie die Webadressen und Webseiten hinzufügen, die Sie als vertrauenswürdig einstufen.

Sie können nur HTTP-/HTTPS-Webadressen zur Liste der vertrauenswürdigen Webadressen hinzufügen. Für die Angabe der Webadressen können Sie Masken verwenden. IP-Adressen können nicht mit Masken beschrieben werden. Standardmäßig ist die Liste leer.

Sie können beim Erstellen einer Adressmaske das Sternchen (*) als Platzhalter für ein oder mehrere Zeichen verwenden. Wenn Sie also die Adressmaske *abc* eingeben, wird sie auf alle Webressourcen angewendet, welche die Sequenz abc enthalten (z. B. www.virus.com/download_virus/page_0-9abcdef.html). Um das Sternchen als Zeichen und nicht als Maske in die Adressmaske aufzunehmen, geben Sie das Zeichen * zweimal ein (z. B. wird mit www.virus.com/**/page_0-9abcdef.html der Link www.virus.com/*/page_0- 9abcdef.html dargestellt).

Sie können die Webadressen in der Liste hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Webadresse"

In diesem Fenster können Sie Webadressen oder eine Maske für Webadressen hinzufügen, die Sie als vertrauenswürdig einstufen.

Sie können nur HTTP-/HTTPS-Webadressen zur Liste der vertrauenswürdigen Webadressen hinzufügen. Für die Angabe der Webadressen können Sie Masken verwenden. IP-Adressen können nicht mit Masken beschrieben werden.

Sie können beim Erstellen einer Adressmaske das Sternchen (*) als Platzhalter für ein oder mehrere Zeichen verwenden. Wenn Sie also die Adressmaske *abc* eingeben, wird sie auf alle Webressourcen angewendet, welche die Sequenz abc enthalten (z. B. www.virus.com/download_virus/page_0-9abcdef.html). Um das Sternchen als Zeichen und nicht als Maske in die Adressmaske aufzunehmen, geben Sie das Zeichen * zweimal ein (z. B. wird mit www.virus.com/**/page_0-9abcdef.html der Link www.virus.com/*/page_0- 9abcdef.html dargestellt).

Fenster "Untersuchungseinstellungen"

In diesem Fenster können Sie die Einstellungen für die Untersuchung des eingehenden Datenverkehrs durch die Komponente "Schutz vor Web-Bedrohungen" konfigurieren.

Einstellungen für den Schutz vor Web-Bedrohungen

Einstellung	Beschreibung
Schädliche Objekte erkennen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Überprüfung von Links gegen Datenbanken mit bösartigen Webadressen. Das Kontrollkästchen ist standardmäßig aktiviert.
Phishing-Links erkennen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Überprüfung von Links gegen Datenbanken mit Phishing-Adressen. Das Kontrollkästchen ist standardmäßig aktiviert.
Heuristische Analyse zum Erkennen von Phishing-Links verwenden	Dieses Kontrollkästchen aktiviert oder deaktiviert die Verwendung der heuristischen Analyse zur Erkennung von Phishing-Links. Dieses Kontrollkästchen ist verfügbar und standardmäßig aktiviert, wenn das Kontrollkästchen **Phishing-Links erkennen** aktiviert ist.
Adware erkennen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Überprüfung von Links gegen die Datenbanken von Adware-Webadressen. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Legale Programme erkennen, die von Angreifern zur Beschädigung von Geräten oder Daten ausgenutzt werden können	Dieses Kontrollkästchen aktiviert oder deaktiviert die Überprüfung von Links gegen die Datenbanken legitimer Anwendungen, mit denen Hacker Geräte oder Daten beschädigen können. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Schutz vor Web-Bedrohungen über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie den Schutz vor Web-Bedrohungen mithilfe der vordefinierten Aufgabe "Schutz vor Web-Bedrohungen" (*Web_Threat_Protection*) verwalten.

Die Aufgabe wird automatisch gestartet, wenn einer der unterstützten Browser im Betriebssystem installiert ist und die lokale Verwaltung der Einstellungen für den Schutz vor Web-Bedrohungen auf dem Gerät zugelassen ist (die Richtlinie wird nicht angewendet oder das "Schloss" ist in den Richtlinieneigenschaften nicht gesetzt).

Sie können diese Aufgabe manuell starten und anhalten. Sie können die Einstellungen für den Schutz vor Web-Bedrohungen konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zum Schutz vor Web-Bedrohungen ändern.

Einstellungen der Aufgabe zum Schutz vor Web-Bedrohungen

Einstellung	Beschreibung	Werte
`ActionOnDetect`	Legt die Aktion fest, die für ein infiziertes Objekt ausgeführt werden soll, das im Web-Datenverkehr gefunden wird.	`Notify` – Den Download des erkannten Objekts erlauben, eine Benachrichtigung über den Zugriffsversuch anzeigen und einen Protokolleintrag mit Informationen zum infizierten Objekt erstellen. `Block` (Standardwert) – Den Zugriff auf das erkannte Objekt blockieren, eine Benachrichtigung über den blockierten Zugriffsversuch anzeigen und einen Protokolleintrag mit Informationen zum infizierten Objekt erstellen.
`CheckMalicious`	Aktiviert oder deaktiviert die Untersuchung von Links gegen Datenbanken mit bösartigen Webadressen.	`Yes` (Standardwert) – Prüfen, ob Links in der Datenbank für bösartige Links aufgeführt sind. `No` – Nicht prüfen, ob Links in der Datenbank für bösartige Links aufgeführt sind.
`CheckPhishing`	Aktiviert oder deaktiviert die Untersuchung von Links gegen Datenbanken mit Phishing-Webadressen.	`Yes` (Standardwert) – Prüfen, ob Links in der Datenbank für Phishing-Links aufgeführt sind. `No` –Nicht prüfen, ob Links in der Datenbank für Phishing-Links aufgeführt sind.
`UseHeuristicForPhishing`	Aktiviert oder deaktiviert die Verwendung der heuristischen Analyse, um Webseiten auf Phishing-Links zu untersuchen.	`Yes` (Standardwert) – Heuristische Analyse zum Erkennen von Phishing-Links verwenden. Bei Angabe dieses Wertes wird als Ebene der heuristischen Analyse `Light` verwendet (die oberflächlichste Untersuchung mit minimaler Systemauslastung). Die Ebene der heuristischen Analyse kann für die Aufgabe zum Schutz vor Web-Bedrohungen nicht geändert werden. `No` – Heuristische Analyse zum Erkennen von Phishing-Links nicht verwenden.
`CheckAdware`	Aktiviert oder deaktiviert die Untersuchung von Links gegen Datenbanken von Adware-Webadressen.	`Yes` – Prüfen, ob Links in der Datenbank für Adware-Links aufgeführt sind. `No` (Standardwert) – Prüfen, ob Links in der Datenbank für Webadressen mit Werbeinhalten aufgeführt sind.
`CheckOther`	Aktiviert oder deaktiviert die Untersuchung von Links gegen Datenbanken von Webadressen, die legitime Anwendungen enthalten, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können.	`Yes` – Untersucht, ob Links in den Datenbanken von Webadressen aufgeführt sind, die legitime Anwendungen enthalten, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können.

		`No` (Standardwert) – Untersucht nicht, ob Links in den Datenbanken von Webadressen aufgeführt sind, die legitime Anwendungen enthalten, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können.
`UseTrustedAddresses`	Aktiviert und deaktiviert die Verwendung einer Liste vertrauenswürdiger Webadressen. Die App untersucht vertrauenswürdige Webadressen nicht auf Viren und andere schädliche Objekte. Sie können vertrauenswürdige Webadressen mit dem Parameter `TrustedAddresses.item_#` angeben.	`Yes` (Standardwert) – Eine Liste mit vertrauenswürdigen Webadressen verwenden. `No` – Keine Liste mit vertrauenswürdigen Webadressen verwenden.
`TrustedAddresses.item_#`	Legt die vertrauenswürdigen Webadressen fest.	Der Standardwert ist nicht angegeben. Für die Angabe der Webadressen können Sie Masken verwenden. Sie können beim Erstellen einer Adressmaske das Sternchen (*) als Platzhalter für ein oder mehrere Zeichen verwenden. Wenn Sie also die Adressmaske *abc* eingeben, wird sie auf alle Webressourcen angewendet, welche die Sequenz abc enthalten (z. B. www.virus.com/download_virus/page_0-9abcdef.html). Um das Sternchen als Zeichen und nicht als Maske in die Adressmaske aufzunehmen, geben Sie das Zeichen * zweimal ein (z. B. wird mit www.virus.com/**/page_0-9abcdef.html der Link www.virus.com/*/page_0-9abcdef.html dargestellt). IP-Adressen können nicht mit Masken beschrieben werden.

Untersuchung geschützter Verbindungen

Die Einstellungen zur Untersuchung geschützter Verbindungen werden bei der Ausführung der Komponenten Schutz vor Web-Bedrohungen und Web-Kontrolle verwendet. Die Komponente zum Schutz vor Web-Bedrohungen kann den über sichere Verbindungen übertragenen Netzwerkverkehr entschlüsseln und untersuchen. Standardmäßig ist die Untersuchung geschützter Verbindungen aktiviert.

Sie können die Untersuchung geschützter Verbindungen aktivieren und deaktivieren sowie Untersuchungseinstellungen konfigurieren:

- Wählen Sie die Aktion aus, die die App ausführen soll, wenn sie ein nicht vertrauenswürdiges Zertifikat erkennt.
- Wählen Sie die Aktion aus, die die App ausführen soll, wenn auf einer Website ein Fehler bei der Untersuchung der geschützten Verbindung auftritt.
- Aktivieren und deaktivieren Sie die Internetnutzung bei der Untersuchung von Zertifikaten.
- Zeigen Sie eine Liste vertrauenswürdiger Domänen an und konfigurieren Sie sie. Die App untersucht keine verschlüsselten Verbindungen, die beim Aufruf bestimmter Domänen hergestellt wurden.
- Konfigurieren Sie die Zertifikate, welche die App während der Untersuchung geschützter Verbindungen als vertrauenswürdig erachten soll.
- Konfigurieren Sie die Liste der von der App gesteuerten Netzwerkports. Sie können bestimmte Netzwerkports oder Bereiche von Netzwerkports angeben, die untersucht werden sollen.

Beim Ändern der Einstellungen zur Untersuchung geschützter Verbindungen generiert die App das Ereignis *NetworkSettingsChanged*.

Untersuchung geschützter Verbindungen in der Web Console konfigurieren

In der Web Console können Sie Einstellungen der Untersuchung geschützter Verbindungen in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen** → **Allgemeine Einstellungen** →**Netzwerkeinstellungen**).

Einstellungen der Untersuchung geschützter Verbindungen

Einstellung	Beschreibung
Untersuchung geschützter Verbindungen aktiviert / deaktiviert	Dieser Schalter aktiviert oder deaktiviert die Untersuchung geschützter Verbindungen. Der Schalter ist standardmäßig aktiviert.
Vertrauenswürdige Stammzertifikate	Wenn Sie auf den Link **Vertrauenswürdige Stammzertifikate verwalten** klicken, wird das Fenster **Vertrauenswürdige Stammzertifikate** geöffnet, in dem Sie die Liste der vertrauenswürdigen Zertifikate konfigurieren können. Vertrauenswürdige Zertifikate werden bei der Untersuchung geschützter Verbindungen verwendet.
Wechsel zu einer Domäne, deren Zertifikat nicht vertrauenswürdig ist	Sie können die Aktion auswählen, die von der App ausgeführt werden soll, wenn zu einer Domäne mit einem nicht vertrauenswürdigen Zertifikat gewechselt wird: • **Erlauben** (Standardwert) – Verbindung zu einer Domäne mit einem nicht vertrauenswürdigen Zertifikat zulassen.

	• **Blockieren** – Verbindung zu einer Domäne mit einem nicht vertrauenswürdigen Zertifikat blockieren.
Wechsel zu einer Domäne mit fehlerhafter Untersuchung der geschützten Verbindung	Sie können die Aktion auswählen, die von der App ausgeführt werden soll, wenn zu einer Domäne gewechselt wird, deren Untersuchung der geschützten Verbindung einen Fehler ausgegeben hat: • **Erlauben und Website zu Ausschlüssen hinzufügen** (Standardwert) – Fügt die Domäne, die zu dem Fehler geführt hat, zur Liste der Domänen mit Untersuchungsfehlern hinzu und überwacht den verschlüsselten Netzwerkdatenverkehr beim Besuch dieser Domäne nicht. • **Blockieren** – Verbindung zu einer Domäne mit Untersuchungsfehler blockieren.
Richtlinie zur Überprüfung von Zertifikaten	Wählen Sie eine Methode für die Überprüfung von Zertifikaten durch die App aus: • **Lokale Überprüfung** – Die App nutzt zur Überprüfung des Zertifikats nicht das Internet. • **Vollständige Überprüfung** (Standardwert) – Die App nutzt das Internet, um die fehlenden Ketten, die zur Überprüfung des Zertifikats erforderlich sind, zu prüfen und herunterzuladen.
Vertrauenswürdige Domänen	Wenn Sie auf den Link **Vertrauenswürdige Domänen konfigurieren** klicken, wird das Fenster **Vertrauenswürdige Domänen** geöffnet, in dem Sie die Liste mit den Namen vertrauenswürdiger Domänen konfigurieren können.
Alle Netzwerkports überwachen	Wenn diese Aktion ausgewählt ist, überwacht die App alle Netzwerkports.
Nur ausgewählte Netzwerkports überwachen	Wenn diese Aktion ausgewählt ist, überwacht die App nur die im Fenster **Überwachte Ports** angegebenen Netzwerkports. Diese Option ist standardmäßig ausgewählt.
Überwachte Ports	Der Link **Einstellungen der Netzwerkports konfigurieren** öffnet das Fenster **Überwachte Ports**, in dem Sie angeben können, welche Netzwerkports die App untersuchen soll.

Fenster "Vertrauenswürdige Zertifikate"

Sie können eine Liste von Zertifikaten konfigurieren, die von der App Kaspersky Endpoint Security als vertrauenswürdig eingestuft werden. Die Liste der vertrauenswürdigen Zertifikate wird bei der Untersuchung verschlüsselter Verbindungen verwendet.

Für jedes Zertifikat werden folgende Informationen angezeigt:

- Zertifikatinhaber
- Seriennummer
- Zertifikataussteller
- Beginn der Gültigkeitsdauer des Zertifikats
- Ende der Gültigkeitsdauer des Zertifikats

- SHA256-Fingerabdruck des Zertifikats

Standardmäßig ist die Liste der Zertifikate leer.

Sie können Zertifikate hinzufügen und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Fenster zum Hinzufügen eines vertrauenswürdigen Zertifikats

In diesem Fenster können Sie ein Zertifikat hinzufügen, das die App Kaspersky Endpoint Security als vertrauenswürdig einstuft.

Mit dem Link **Zertifikat hinzufügen** wird ein Standardfenster zur Dateiauswahl geöffnet. Geben Sie den Pfad zu einer Datei im Format DER oder PEM an, die das Zertifikat enthält.

Nach Auswahl der Zertifikatsdatei werden in diesem Fenster Informationen zum Zertifikat und der Dateipfad angezeigt.

Fenster "Vertrauenswürdige Domänen"

Diese Liste enthält Domänennamen und Masken für Domänennamen, die von der Untersuchung verschlüsselter Verbindungen ausgenommen werden.

Beispiel: `*example.com`. Der Wert `*example.com/*` ist beispielsweise ungültig, da dafür eine Domänenadresse und keine Webseite erforderlich ist.

Standardmäßig ist die Liste leer.

Sie können die Domänen in der Liste der vertrauenswürdigen Domänen hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Überwachte Ports"

Die Tabelle enthält die Netzwerkports, die von der App untersucht werden, wenn im Fenster Netzwerkeinstellungen im Abschnitt **Überwachte Ports** die Option **Nur ausgewählte Netzwerkports überwachen** ausgewählt ist.

Die Tabelle enthält zwei Spalten:

- **Port** – Der überwachte Port.
- **Beschreibung** – Die Beschreibung des überwachten Ports.

In der Tabelle wird standardmäßig eine Liste der Netzwerkports angezeigt, die normalerweise für die Übertragung von E-Mail- und Netzwerkverkehr verwendet werden. Diese Liste der Netzwerkports ist im App-Paket enthalten.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Untersuchung geschützter Verbindungen in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie Einstellungen der Untersuchung geschützter Verbindungen in den Einstellungen der Richtlinie konfigurieren (**Allgemeine Einstellungen** → **Netzwerkeinstellungen**).

Einstellungen der Untersuchung geschützter Verbindungen

Einstellung	Beschreibung
Untersuchung geschützter Verbindungen aktivieren	Dieses Kontrollkästchen aktiviert oder deaktiviert die Untersuchung geschützter Verbindungen. Das Kontrollkästchen ist standardmäßig aktiviert.
Wechsel zu einer Domäne, deren Zertifikat nicht vertrauenswürdig ist	In der Dropdown-Liste können Sie die Aktion auswählen, die von der App ausgeführt werden soll, wenn zu einer Domäne mit einem nicht vertrauenswürdigen Zertifikat gewechselt wird: • **Erlauben** (Standardwert) – Verbindung zu einer Domäne mit einem nicht vertrauenswürdigen Zertifikat zulassen. • **Blockieren** – Verbindung zu einer Domäne mit einem nicht vertrauenswürdigen Zertifikat blockieren.
Wechsel zu einer Domäne mit fehlerhafter	In der Dropdown-Liste können Sie die Aktion auswählen, die von der App ausgeführt werden soll, wenn zu einer Domäne gewechselt wird, deren Untersuchung der geschützten Verbindung einen Fehler ausgegeben hat:

Untersuchung der geschützten Verbindung	• **Domäne zu den Ausschlüssen hinzufügen** (Standardwert) – Fügt die Domäne, die zu dem Fehler geführt hat, zur Liste der Domänen mit Untersuchungsfehlern hinzu und überwacht den verschlüsselten Netzwerkdatenverkehr beim Besuch dieser Domäne nicht. • **Blockieren** – Verbindung zu einer Domäne mit Untersuchungsfehler blockieren.
Richtlinie zur Überprüfung von Zertifikaten	In dieser Dropdown-Liste können Sie eine Methode für die Überprüfung von Zertifikaten durch die App festlegen: • **Lokale Überprüfung** – Die App nutzt zur Überprüfung des Zertifikats nicht das Internet. • **Vollständige Überprüfung** (Standardwert) – Die App nutzt das Internet, um die fehlenden Ketten, die zur Überprüfung des Zertifikats erforderlich sind, zu prüfen und herunterzuladen.
Vertrauenswürdige Domänen	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster Vertrauenswürdige Webadressen öffnet. In diesem Fenster können Sie eine Liste mit den Namen vertrauenswürdiger Domänen konfigurieren.
Vertrauenswürdige Stammzertifikate	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster Vertrauenswürdige Stammzertifikate öffnet. In diesem Fenster können Sie eine Liste mit vertrauenswürdigen Stammzertifikaten konfigurieren. Vertrauenswürdige Zertifikate werden bei der Untersuchung geschützter Verbindungen verwendet.
Einstellungen der Netzwerkports	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster Überwachte Ports öffnet.

Fenster "Vertrauenswürdige Domänen"

Diese Liste enthält Domänennamen und Masken für Domänennamen, die von der Untersuchung verschlüsselter Verbindungen ausgenommen werden.

Beispiel: `*example.com`. Der Wert `*example.com/*` ist beispielsweise ungültig, da dafür eine Domänenadresse und keine Webseite erforderlich ist.

Standardmäßig ist die Liste leer.

Sie können die Domänen in der Liste der vertrauenswürdigen Domänen hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Vertrauenswürdige Zertifikate"

Sie können eine Liste von Zertifikaten konfigurieren, die von der App Kaspersky Endpoint Security als vertrauenswürdig eingestuft werden. Die Liste der vertrauenswürdigen Zertifikate wird bei der Untersuchung verschlüsselter Verbindungen verwendet.

Für jedes Zertifikat werden folgende Informationen angezeigt:

- **Antragsteller** – Der Antragsteller des Zertifikats
- **Seriennummer** – Die Seriennummer des Zertifikats
- **Aussteller** – Der Aussteller des Zertifikats
- **Gültig ab** – Das Startdatum der Gültigkeitsdauer des Zertifikats
- **Gültig bis** – Das Ablaufdatum der Gültigkeitsdauer des Zertifikats
- **SHA256-Fingerabdruck** – Der SHA256-Fingerabdruck des Zertifikats

Standardmäßig ist die Liste der Zertifikate leer.

Sie können Zertifikate hinzufügen und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Fenster "Zertifikat hinzufügen"

In diesem Fenster können Sie ein Zertifikat zur Liste der vertrauenswürdigen Zertifikate hinzufügen. Dafür gibt es folgende Möglichkeiten:

- Pfad der Zertifikatsdatei angeben. Mit der Schaltfläche **Durchsuchen** wird ein Standardfenster für die Dateiauswahl geöffnet. Geben Sie den Pfad zur Datei des DER- oder PEM-Formats an, die das Zertifikat enthält.
- Inhalt der Zertifikatsdatei in das Feld **Zertifikatdetails angeben** kopieren.

Fenster "Überwachte Ports"

Einstellungen der Netzwerkports

Einstellung	Beschreibung
Alle Netzwerkports überwachen	Wenn diese Aktion ausgewählt ist, überwacht die App alle Netzwerkports.
Nur	Wenn diese Aktion ausgewählt ist, überwacht die App nur die in der Tabelle angegebenen

ausgewählte Netzwerkports überwachen	Netzwerkports. Diese Option ist standardmäßig ausgewählt.
Einstellungen der Netzwerkports	Die Tabelle enthält die Netzwerkports, die von der App untersucht werden, wenn die Aktion **Nur angegebene Ports kontrollieren** ausgewählt ist. Die Tabelle enthält zwei Spalten: • **Port** – Der überwachte Port. • **Beschreibung** – Die Beschreibung des überwachten Ports. In der Tabelle wird standardmäßig eine Liste der Netzwerkports angezeigt, die normalerweise für die Übertragung von E-Mail- und Netzwerkverkehr verwendet werden. Diese Liste der Netzwerkports ist im App-Paket enthalten. Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster. Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Untersuchung geschützter Verbindungen über die Befehlszeile konfigurieren

Die Befehlszeile stellt spezielle Verwaltungsbefehle zur Verfügung, um die Einstellungen zur Untersuchung geschützter Verbindungen zu verwalten. Mithilfe von Befehlen zur Verwaltung der Einstellungen zur Untersuchung geschützter Verbindungen können Sie Folgendes tun:

- Einstellungen zur Untersuchung geschützter Verbindungen konfigurieren.
- Ausschlüsse von der Untersuchung geschützter Verbindungen anzeigen.
- Die Liste der Domänen löschen, die die App automatisch von der Untersuchung ausgeschlossen hat.
- Die Liste der Zertifikate verwalten, die die App als vertrauenswürdig erachtet.

Einstellungen zur Untersuchung geschützter Verbindungen anzeigen und ändern

Mit speziellen Verwaltungsbefehlen können Sie die Einstellungen zur Untersuchung geschützter Verbindungen anzeigen und ändern:

- Sie können die aktuellen Werte der Einstellungen zur Untersuchung geschützter Verbindungen in die Konsole oder in eine Konfigurationsdatei ausgeben. Mit dieser Datei können Sie Einstellungen ändern.

- Sie können alle Einstellungen der Untersuchung geschützter Verbindungen mithilfe der Konfigurationsdatei ändern, die die Einstellungen enthält. Sie können die Konfigurationsdatei mit dem Befehl zur Ausgabe der Einstellungen zur Untersuchung geschützter Verbindungen abrufen.

- Sie können einzelne Einstellungen mithilfe von Befehlszeilenschaltern im Format `<Name der Einstellung>=<Wert der Einstellung>` ändern. Mit dem Befehl zur Ausgabe der Einstellungen zur Untersuchung geschützter Verbindungen können Sie die aktuellen Werte der Einstellungen abrufen.

Um die aktuellen Werte der Einstellungen zur Untersuchung geschützter Verbindungen in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-net-settings [--json]
```

Wobei gilt: `--json` – Gibt Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Um die aktuellen Werte der Einstellungen zur Untersuchung geschützter Verbindungen in die Datei auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-net-settings --file <Pfad der Konfigurationsdatei> [--json]
```

Wobei gilt:

- `--file <Pfad der Konfigurationsdatei>` – Pfad der Datei, in der die Einstellungen der Untersuchung geschützter Verbindungen gespeichert werden. Wenn Sie den Dateinamen eingeben, ohne einen Dateipfad vorzugeben, wird die Datei im aktuellen Verzeichnis erstellt. Ist unter dem gewünschten Pfad bereits eine Datei mit gleichem Namen vorhanden, wird diese überschreiben. Falls das von Ihnen vorgegebene Verzeichnis auf der Festplatte nicht existiert, wird die Datei nicht erstellt.

- `--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

So ändern Sie die Werte der Einstellungen zur Untersuchung geschützter Verbindungen mithilfe einer Konfigurationsdatei:

1. Geben Sie die allgemeinen App-Einstellungen wie oben beschrieben in eine Konfigurationsdatei aus.

2. Ändern Sie die Werte der erforderlichen Einstellungen in der Datei und speichern Sie die Änderungen.

3. Führen Sie den Befehl aus:

   ```
   kesl-control --set-net-settings --file <Pfad der Konfigurationsdatei> [--json]
   ```

   Wobei gilt:

   - `--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei mit den Einstellungen zur Untersuchung geschützter Verbindungen.

   - `--json` – Importiert die Einstellungen aus einer Konfigurationsdatei im JSON-Format in die App. Wenn Sie den Schalter `--json` nicht angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Alle in der Datei angegebenen Werte der Einstellungen zur Untersuchung geschützter Verbindungen werden in die App importiert.

Um die Werte der Einstellungen zur Untersuchung geschützter Verbindungen über die Befehlszeile zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-net-settings <Name der Einstellung>=<Wert der Einstellung> [<Name der Einstellung>=<Wert der Einstellung>]
```

Wobei gilt: `<Name der Einstellung>=<Wert der Einstellung>` – Name und Wert einer der Einstellungen zur Untersuchung geschützter Verbindungen.

Die Werte der angegebenen Einstellungen zur Untersuchung geschützter Verbindungen werden geändert.

Ausschlüsse von der Untersuchung geschützter Verbindungen anzeigen

Sie können die folgenden Listen mit Ausschlüssen von der Untersuchung geschützter Verbindungen anzeigen:

- Liste der vom Benutzer hinzugefügten Ausschlüsse;
- Liste der von der App hinzugefügten Ausschlüsse;
- Liste der von den App-Datenbanken abgerufenen Ausschlüsse.

Um die Liste der vom Benutzer hinzugefügten Ausschlüsse von der Untersuchung geschützter Verbindungen anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control -N --query user
```

Um die Liste der von der App hinzugefügten Ausschlüsse von der Untersuchung geschützter Verbindungen anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control -N --query auto
```

Um die Liste der Ausschlüsse von der Untersuchung geschützter Verbindungen anzuzeigen, die von den App-Datenbanken abgerufen wurden, führen Sie den folgenden Befehl aus:

```
kesl-control -N --query kl
```

Um die Liste der Domänen zu löschen, welche die App automatisch von der Untersuchung ausgeschlossen hat, führen Sie den folgenden Befehl aus:

```
kesl-control -N --clear-web-auto-excluded
```

Liste der vertrauenswürdigen Zertifikate verwalten

Um ein Zertifikat zur Liste der vertrauenswürdigen Zertifikate hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --add-certificate <Pfad des Zertifikats>
```

Wobei gilt:

`<Pfad des Zertifikats>` – Pfad der Zertifikatsdatei, die Sie hinzufügen möchten, im PEM- oder DER-Format.

Um ein Zertifikat aus der Liste der vertrauenswürdigen Zertifikate zu entfernen, führen Sie den folgenden Befehl aus:

```
kesl-control --remove-certificate <Zertifikatinhaber>
```

Um die Liste der vertrauenswürdigen Zertifikate anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --list-certificates
```

Für jedes Zertifikat werden folgende Informationen angezeigt:

- Zertifikatinhaber
- Seriennummer
- Zertifikataussteller
- Beginn der Gültigkeitsdauer des Zertifikats
- Ende der Gültigkeitsdauer des Zertifikats
- SHA256-Fingerabdruck des Zertifikats

Schutz vor Netzwerkbedrohungen

Die Komponente "Schutz vor Netzwerkbedrohungen" untersucht den eingehenden Netzwerkdatenverkehr auf Aktivitäten, die für Netzwerkangriffe typisch sind.

Diese Funktionalität wird im KESL-Container nicht unterstützt.

Die App untersucht den eingehenden Datenverkehr für TCP-Ports, deren Nummern Kaspersky Endpoint Security aus den aktuellen App-Datenbanken erhält.

Zur Untersuchung des Netzwerkverkehrs akzeptiert die Aufgabe zum Schutz vor Netzwerkbedrohungen Verbindungen von allen Ports, deren Nummern sie aus den Datenbanken der App erhält. Bei der Untersuchung des Netzwerkes können auf Geräten geöffnete Ports auftauchen, die von keiner Anwendung auf diesem System verwendet werden. Es wird empfohlen, nicht verwendetet Ports mittels Firewall zu schließen.

Aktuelle Verbindungen für abgefangene TCP-Ports werden zurückgesetzt, wenn der Schutz vor Netzwerkbedrohungen aktiviert ist.

Wenn der Schutz vor Netzwerkbedrohungen aktiviert ist und ein versuchter Netzwerkangriff auf ein geschütztes Gerät erkannt wird, blockiert die App die Netzwerkaktivität des angreifenden Geräts und generiert das Ereignis *Netzwerkangriff erkannt*. Das Ereignis enthält Informationen über das angreifende Gerät.

Standardmäßig wird der Netzwerkverkehr des angreifenden Geräts für eine Stunde blockiert. Nach Ablauf der Sperrzeit entsperrt die App das Gerät.

Der Schutz vor Netzwerkbedrohungen ist standardmäßig aktiviert, wenn die Einstellungen für den Schutz vor Netzwerkbedrohungen auf dem Gerät durch eine Richtlinie festgelegt werden. Wenn auf das Gerät lokal konfigurierte Einstellungen angewendet werden, ist der Schutz vor Netzwerkbedrohungen standardmäßig deaktiviert.

Sie können den Schutz vor Netzwerkbedrohungen ein- und ausschalten und auch Schutzeinstellungen konfigurieren:

- Wählen Sie die Aktion aus, die die App ausführen soll, wenn sie eine für Netzwerkangriffe typische Netzwerkaktivität erkennt.
- Aktivieren und deaktivieren Sie das Blockieren der Netzwerkaktivität, wenn ein versuchter Netzwerkangriff erkannt wird.
- Legen Sie die Dauer der Blockierung des angreifenden Geräts fest.
- Konfigurieren Sie eine Liste von IP-Adressen, deren Netzwerkaktivität nicht durch die App blockiert wird.

Mithilfe der Befehle zur Verwaltung blockierter Geräte in der Befehlszeile können Sie die Liste der blockierten Geräte anzeigen und diese Geräte manuell entsperren. Kaspersky Security Center verfügt über keine Tools zur Überwachung und Verwaltung blockierter Geräte, mit Ausnahme der Ereignisse *Netzwerkangriff erkannt*.

Kaspersky Endpoint Security fügt zur Liste der Tabelle mangle der Tools iptables und ip6tables eine spezielle Erlaubniskette der Regeln kesl_bypass hinzu, die es erlaubt, den Datenverkehr von der Untersuchung durch die App auszuschließen. Wenn in der Kette Ausschlussregeln für den Datenverkehr konfiguriert sind, wirken sich diese auf die Aufgabe "Schutz vor Netzwerkbedrohungen" aus. Um beispielsweise ausgehenden HTTP-Verkehr auszuschließen, müssen Sie den folgenden Befehl hinzufügen: `iptables -t mangle -I kesl_bypass -m tcp -p tcp --dport http -j ACCEPT`.

Schutz vor Netzwerkbedrohungen in der Web Console konfigurieren

In der Web Console können Sie Einstellungen des Schutzes vor Netzwerkbedrohungen in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen** → **Basisschutz** → **Schutz vor Netzwerkbedrohungen**).

Einstellungen der Komponente "Schutz vor Netzwerkbedrohungen"

Einstellung	Beschreibung
Schutz vor Netzwerkbedrohungen aktiviert/deaktiviert	Dieser Schalter aktiviert bzw. deaktiviert den Schutz vor Netzwerkbedrohungen. Der Schalter ist standardmäßig aktiviert.
Aktion beim Erkennen einer Bedrohung	Zu ergreifende Maßnahmen, wenn eine Netzwerkaktivität erkannt wird, die auf Netzwerkangriffe hinweist: • **Informieren** Sie den Benutzer. Die App lässt Netzwerkaktivität zu und protokolliert Informationen über erkannte Netzwerkaktivität. • **Blockieren** Sie Netzwerkaktivität vom angreifenden Gerät und protokollieren Sie Informationen über erkannte Netzwerkaktivität (Standardwert).
Blockieren angreifender Geräte aktiviert/deaktiviert	Dieser Schalter aktiviert und deaktiviert das Blockieren der Netzwerkaktivität, wenn ein versuchter Netzwerkangriff erkannt wird. Der Schalter ist standardmäßig aktiviert.
Angreifendes Gerät blockieren für (Min)	In diesem Feld können Sie angeben, wie lange ein angreifendes Gerät blockiert werden soll (in Minuten). Nach Ablauf der angegebenen Zeit erlaubt die App Kaspersky Endpoint Security die Netzwerkaktivität von diesem Gerät aus. Mögliche Werte sind ganze Zahlen zwischen 1 und 32768. Standardwert: 60.
Ausschlüsse	Die Tabelle enthält eine Liste von IP-Adressen, von denen Netzwerkangriffe nicht blockiert werden. Standardmäßig ist die Liste leer. Sie können die IP-Adressen in der Tabelle hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

	Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "IP-Adresse"

Sie können IP-Adressen hinzufügen und ändern, von denen ausgehende Netzwerkangriffe nicht von der App Kaspersky Endpoint Security blockiert werden.

IP-Adressen

Einstellung	Beschreibung
IP-Adresse eingeben	Eingabefeld für eine IP-Adresse. Sie können IP-Adressen in den Formaten IPv4 und IPv6 eingeben.

Schutz vor Netzwerkbedrohungen in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen des Schutzes vor Netzwerkbedrohungen in den Einstellungen der Richtlinie konfigurieren (**Basisschutz → Schutz vor Netzwerkbedrohungen**).

Einstellungen der Komponente "Schutz vor Netzwerkbedrohungen"

Einstellung	Beschreibung
Schutz vor Netzwerkbedrohungen aktivieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Komponente "Schutz vor Netzwerkbedrohungen". Das Kontrollkästchen ist standardmäßig aktiviert.
Aktion beim Erkennen einer Bedrohung	Zu ergreifende Maßnahmen, wenn eine Netzwerkaktivität erkannt wird, die auf Netzwerkangriffe hinweist: • **Informieren** Sie den Benutzer. Die App lässt Netzwerkaktivität zu und protokolliert Informationen über erkannte Netzwerkaktivität. • **Blockieren** Sie Netzwerkaktivität vom angreifenden Gerät und protokollieren Sie Informationen über erkannte Netzwerkaktivität (Standardwert).
Blockieren von angreifenden Geräten aktivieren	Dieses Kontrollkästchen aktiviert und deaktiviert das Blockieren der Netzwerkaktivität, wenn ein versuchter Netzwerkangriff erkannt wird. Das Kontrollkästchen ist standardmäßig aktiviert.
Angreifendes Gerät blockieren für (Min)	In diesem Feld können Sie angeben, wie lange ein angreifendes Gerät blockiert werden soll (in Minuten). Nach Ablauf der angegebenen Zeit erlaubt die App Kaspersky Endpoint Security die Netzwerkaktivität von diesem Gerät aus. Mögliche Werte sind ganze Zahlen zwischen 1 und 32768. Standardwert: 60.
Ausschlüsse	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster Ausschlüsse öffnet. In diesem Fenster können Sie eine Liste von IP-Adressen angeben, von denen keine Netzwerkangriffe blockiert werden sollen.

Fenster "Ausschlüsse"

In diesem Fenster können Sie IP-Adressen hinzufügen, von denen ausgehende Netzwerkangriffe nicht blockiert werden.

Standardmäßig ist die Liste leer.

Sie können die IP-Adressen in der Liste hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "IP-Adresse"

Sie können IP-Adressen hinzufügen und ändern, von denen ausgehende Netzwerkangriffe nicht von der App Kaspersky Endpoint Security blockiert werden.

IP-Adressen

Einstellung	Beschreibung
IP-Adresse eingeben	Eingabefeld für eine IP-Adresse. Sie können IP-Adressen in den Formaten IPv4 und IPv6 eingeben.

Schutz vor Netzwerkbedrohungen über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie den Schutz vor Netzwerkbedrohungen mithilfe der vordefinierten Aufgabe "Schutz vor Netzwerkbedrohungen" (*Network_Threat_Protection*) verwalten.

Die Aufgabe zum Schutz vor Netzwerkbedrohungen wird standardmäßig nicht gestartet. Sie können diese Aufgabe manuell starten und anhalten.

Sie können die Einstellungen für den Schutz vor Netzwerkbedrohungen konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zum Schutz vor Netzwerkbedrohungen ändern.

Einstellungen der Aufgabe zum Schutz vor Netzwerkbedrohungen

Einstellung	Beschreibung	Werte
`ActionOnDetect`	Zu ergreifende Maßnahmen, wenn eine Netzwerkaktivität	`Notify` – Netzwerkaktivität zulassen und Informationen über erkannte

	erkannt wird, die auf Netzwerkangriffe hinweist. Wenn Sie diese Einstellung von `Block` auf `Notify` ändern, wird die Liste der blockierten Geräte gelöscht.	Netzwerkaktivitäten protokollieren. Wenn dieser Wert angegeben wird, wird der Wert des Parameters `BlockAttackingHosts` ignoriert. `Block` (Standardwert) – Netzwerkaktivität blockieren und Informationen darüber protokollieren.
`BlockAttackingHosts`	Blockieren der Netzwerkaktivität von angreifenden Geräten.	`Yes` (Standardwert) – Netzwerkaktivität angreifender Geräte blockieren. `No` – Netzwerkaktivität angreifender Geräte nicht blockieren. Wenn dieser Wert angegeben und der Parameter `ActionOnDetect` auf `Block` gesetzt ist, blockiert die App die Netzwerkaktivität des angreifenden Geräts, fügt das Gerät aber nicht zur Liste der blockierten Geräte hinzu.
`BlockDurationMinutes`	Legt fest, wie lange angreifende Geräte blockiert werden (in Minuten).	1 – 32768 Standardwert: 60.
`UseExcludeIPs`	Verwendung einer Liste von IP-Adressen, deren Netzwerkaktivität nicht blockiert wird, wenn ein Netzwerkangriff erkannt wird. Die App protokolliert nur Informationen zu gefährlichen Aktivitäten von diesen Geräten. Sie können IP-Adressen mithilfe des Parameters `ExcludeIPs.item_#` zur Liste mit Ausschlüsse hinzufügen.	`Yes` – Liste mit Ausschlüssen für IP-Adressen wird verwendet. `No` (Standardwert) – Liste mit Ausschlüssen für IP-Adressen wird nicht verwendet.
`ExcludeIPs.item_#`	Gibt eine IP-Adresse an, deren Netzwerkaktivität nicht durch die App blockiert wird. Standardmäßig ist die Liste leer.	`d.d.d.d` – IPv4-Adresse, wobei d eine Dezimalzahl von 0 bis 255 ist. `d.d.d.d/p` – Subnetz von IPv4-Adressen, wobei p eine Zahl von 0 bis 32 ist. `x:x:x:x:x:x:x:x` – IPv6-Adresse, wobei x eine hexadezimale Zahl von 0 bis ffff ist. `x:x:x:x::0/p` – Subnetz von IPv6-Adressen, wobei p eine Zahl von 0 bis 64 ist. Der Standardwert ist nicht angegeben.

Schutz vor bösartiger Remote-Verschlüsselung

Die Komponente "Schutz vor Verschlüsselung" ermöglicht Ihnen, Ihre Dateien in den lokalen Verzeichnissen mit Netzwerkzugang durch SMB-/NFS-Protokolle vor bösartiger Remote-Verschlüsselung zu schützen.

Um die Komponente nutzen zu können, benötigen Sie eine Lizenz, in der diese Funktionalität enthalten ist.

Diese Funktionalität wird im KESL-Container nicht unterstützt.

Wenn der Schutz vor Verschlüsselung aktiviert ist, prüft Kaspersky Endpoint Security die Aktionen von Remote-Geräten mit Dateiressourcen, die sich in freigegebenen Netzwerkverzeichnissen des geschützten Geräts befinden, auf bösartige Verschlüsselung. Wenn die App die Aktionen eines Remote-Geräts, das auf freigegebene Netzwerkressourcen zugreift, als bösartige Verschlüsselung interpretiert, erstellt und aktiviert die App eine Regel für die Firewall des Betriebssystems, die den Netzwerkverkehr vom gefährdeten Gerät blockiert. Das kompromittierte Gerät wird zur Liste der nicht vertrauenswürdigen Geräte hinzugefügt und der Zugriff auf freigegebene Netzwerkverzeichnisse für alle nicht vertrauenswürdigen Geräte wird blockiert. Die App generiert das Ereignis *Verschlüsselung erkannt*, das Informationen über das gefährdete Gerät enthält.

Standardmäßig blockiert die App den Zugriff von nicht vertrauenswürdigen Computern auf freigegebene Netzwerkordner für 30 Minuten. Nach Ablauf der Sperrzeit entfernt die App das gefährdete Gerät aus der Liste der nicht vertrauenswürdigen Geräte und der Zugriff des Geräts auf freigegebene Netzwerkordner wird automatisch wiederhergestellt.

Firewall-Regeln, die von der Komponente "Schutz vor Verschlüsselung" erstellt wurden, können nicht mithilfe des Tools "iptables" gelöscht werden, da die App die Regeln jede Minute wiederherstellt.

Standardmäßig ist der Schutz vor bösartiger Remote-Verschlüsselung deaktiviert.

Sie können den Schutz vor bösartiger Verschlüsselung ein- und ausschalten und auch Schutzeinstellungen konfigurieren:

- Wählen Sie die Aktion aus, die von der App ausgeführt werden soll, wenn eine Verschlüsselung erkannt wird: Den Benutzer informieren oder das Gerät blockieren, das eine böswillige Verschlüsselung durchführt.

  Wenn die Aktion *Informieren* ausgewählt wurde, untersucht die App die Aktionen von Remote-Geräten mit freigegebenen Netzwerkordnern trotzdem auf bösartige Verschlüsselung, wenn die Aufgabe zum Schutz vor Verschlüsselung ausgeführt wird. Sollte eine bösartige Verschlüsselung erkannt werden, wird das Ereignis *Verschlüsselung erkannt* erstellt, das kompromittierte Gerät wird jedoch nicht blockiert.

- Legen Sie die Dauer für die Blockierung eines nicht vertrauenswürdigen Geräts fest.

- Geben Sie Dateien und Verzeichnisse an, die die App vor bösartiger Verschlüsselung schützt.

- Geben Sie Dateien und Verzeichnisse an, die vom Schutz vor bösartiger Verschlüsselung ausgeschlossen sind.

  Die App stuft eine Aktivität nicht als Verschlüsselung ein, wenn die Verschlüsselungsaktivität in Verzeichnissen entdeckt wird, die vom Schutz vor Verschlüsselung ausgeschlossen sind.

Mithilfe der Befehle zur Verwaltung blockierter Geräte in der Befehlszeile können Sie die Liste der blockierten Geräte anzeigen und diese Geräte manuell entsperren. Kaspersky Security Center verfügt über keine Tools zur Überwachung und Verwaltung blockierter Geräte, mit Ausnahme der Ereignisse *Verschlüsselung erkannt*.

Damit die Komponente "Schutz vor Verschlüsselung" ordnungsgemäß ausgeführt werden kann, muss mindestens einer der folgenden Dienste im Betriebssystem installiert sein: Samba oder NFS. Für den NFS-Dienst muss das Paket rpcbind installiert sein.

Die Komponente "Schutz vor Verschlüsselung" wird mit den Protokollen SMB1, SMB2, SMB3, NFS3, TCP/UDP und IP/IPv6 korrekt ausgeführt. Die Protokolle NFS2 und NFS4 werden nicht unterstützt. Es wird empfohlen, dass Sie Ihre Server-Einstellungen so konfigurieren, dass NFS2- und NFS4-Protokolle nicht zum Mounten von Ressourcen verwendet werden können.

Kaspersky Endpoint Security blockiert den Zugriff auf die freigegebenen Netzwerkordner erst dann, wenn die Aktivitäten des Geräts als bösartig eingestuft wurden. Es wird daher mindestens eine Datei verschlüsselt, bevor die App eine bösartige Aktivität erkennt.

Schutz vor Verschlüsselung in der Web Console konfigurieren

In der Web Console können Sie Einstellungen des Schutzes vor Verschlüsselung in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen** → **Erweiterter Schutz** → **Schutz vor Verschlüsselung**).

Einstellungen der Komponente "Schutz vor Verschlüsselung"

Einstellung	Beschreibung
Schutz vor Verschlüsselung aktiviert/deaktiviert	Dieser Schalter aktiviert bzw. deaktiviert den Schutz von Dateien in lokalen Verzeichnissen, auf die der Netzwerkzugriff über SMB/NFS-Protokolle möglich ist, vor bösartiger Remote-Verschlüsselung. Der Schalter ist standardmäßig deaktiviert.
Schutzbereiche	Der Link **Schutzbereich konfigurieren** öffnet das Fenster **Schutzbereiche**.
Aktion beim Erkennen einer Verschlüsselung:	Aktion, die Kaspersky Endpoint Security ausführt, wenn es eine schädliche Verschlüsselung erkennt: • **Informieren** des Benutzers. Kaspersky Endpoint Security blockiert das Gerät, das die Verschlüsselung ausführt nicht. Es protokolliert lediglich ein Ereignis über die Erkennung einer bösartigen Verschlüsselung im Ereignisprotokoll. • **Blockieren** des Geräts, das die Verschlüsselung durchführt (Standardeinstellung).
Nicht vertrauenswürdiges Gerät blockieren für (Min)	In diesem Feld können Sie angeben, wie lange ein nicht vertrauenswürdiges Gerät blockiert werden soll (in Minuten). Wenn ein gefährdetes Gerät blockiert wurde und Sie den Wert dieser Einstellung ändern, ändert sich die Dauer, für die das Gerät blockiert ist, nicht. Diese Dauer ist kein dynamischer Wert und wird zum Zeitpunkt der Blockierung berechnet. Mögliche Werte sind ganze Zahlen zwischen 1 und 4294967295. Standardwert: 30.
Ausschlüsse	Der Link **Ausschlüsse anpassen** öffnet das Fenster **Ausschlussbereiche**.
Ausschlüsse nach Maske	Der Link **Ausschlüsse nach Maske anpassen** öffnet das Fenster **Ausschlüsse nach Maske**.

Fenster "Schutzbereiche"

Die Tabelle enthält die Schutzbereiche der Komponente "Schutz vor Verschlüsselung". Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle einen Untersuchungsbereich, der alle Verzeichnisse des lokalen Dateisystems umfasst.

Einstellungen des Schutzbereichs

Einstellung	Beschreibung
Name des Bereichs	Name des Schutzbereichs.
Pfad	Pfad zum geschützten Verzeichnis.
Status	Der Status gibt an, ob die App diesen Bereich während ihrer Ausführung untersucht.

Sie können Elemente in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.

Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Kaspersky Endpoint Security schützt Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Liste der Bereiche angeben sind. Um bei Bedarf für das Unterverzeichnis andere Sicherheitseinstellungen festzulegen als für das übergeordnete Verzeichnis, platzieren Sie erforderlichenfalls das Unterverzeichnis in der Liste über dem übergeordneten Verzeichnis.

Fenster zum Hinzufügen des Schutzbereichs

In diesem Fenster können Sie den Schutzbereich der Komponente "Schutz vor Verschlüsselung" hinzufügen und bearbeiten.

Einstellungen des Schutzbereichs

Einstellung	Beschreibung

Name des Bereichs	Eingabefeld für den Namen des Schutzbereichs. Dieser Name wird in der Tabelle im Fenster **Schutzbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung dieses Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, verarbeitet die App diesen Schutzbereich während der Ausführung der Komponente. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die App diesen Schutzbereich während der Ausführung der Komponente nicht. Sie können diesen Bereich zu einem späteren Zeitpunkt zu den Betriebseinstellungen der Komponente hinzufügen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	In der Dropdown-Liste können Sie den Typ des Dateisystems auswählen: • **Lokal** (Standardwert) – Lokale Verzeichnisse. • **Freigegeben** – Ressourcen von Server-Dateisystemen, die über das Samba- oder NFS-Protokoll zugänglich sind. • **Alle freigegebenen** – Alle Ressourcen des Server-Dateisystems, die über das Samba- oder NFS-Protokoll zugänglich sind.
Zugriffsprotokoll	In der Dropdown-Liste können Sie das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. Diese Dropdown-Liste ist verfügbar, wenn in der Dropdown-Liste für Dateisysteme das Element **Freigegeben** ausgewählt ist.
Pfad	Eingabefeld für den Pfad des Verzeichnisses, das in den Schutzbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

	Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Lokal** ausgewählt ist. Das Feld darf nicht leer sein. Standardmäßig ist der Pfad **/** angegeben (Root-Verzeichnis).
Masken	Diese Liste enthält die Masken der Objektnamen, die von der App während der Ausführung der Komponente zum Schutz vor Verschlüsselung untersucht werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster. Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Ausschlussbereiche"

Die Tabelle enthält Bereiche mit Ausschlüsse von der Untersuchung. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der App angewendet wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster zum Hinzufügen des Ausschlussbereichs

In diesem Fenster können Sie einen neuen Ausschlussbereich hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster **Ausschlussbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss des Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, wird dieser Bereich während der Ausführung der App von der Untersuchung oder vom Schutz ausgeschlossen. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich während der Ausführung der App in die Untersuchung oder den Schutz eingeschlossen. Im Folgenden können Sie diesen Bereich von der Untersuchung oder dem Schutz ausschließen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	In der Dropdown-Liste können Sie den Typ des Dateisystems auswählen, auf dem sich die Verzeichnisse befinden, die Sie zu den Ausschlüssen von der Untersuchung hinzufügen möchten: • **Lokal** – Lokale Verzeichnisse. • **Mounted** – Remote-Verzeichnisse, die auf dem Gerät eingebunden sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind.
Zugriffsprotokoll	In der Dropdown-Liste können Sie das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind. Diese Dropdown-Liste ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** ausgewählt ist.
Pfad	Eingabefeld für den Pfad des Verzeichnisses, das in den Ausschlussbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken und Tags verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

	Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Als Pfad ist standardmäßig **/** angegeben: Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Lokal** ausgewählt ist.
Name der freigegebenen Ressource	Eingabefeld für den Namen der freigegebenen Ressource des Dateisystems, auf der sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten: Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste **Zugriffsprotokoll** das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Untersuchung ausgeschlossen werden. Die Masken werden nur innerhalb des Verzeichnisses übernommen, das im Eingabefeld **Pfad** angegeben ist. Standardmäßig enthält die Liste die Maske ***** (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen. Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist. Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Maske"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren. Die App untersucht keine Dateien, deren Namen die angegebenen Masken enthalten. Standardmäßig ist die Liste mit Masken leer.

Sie können Masken hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist.

Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Schutz vor Verschlüsselung in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie Einstellungen des Schutzes vor Verschlüsselung in den Einstellungen der Richtlinie konfigurieren (**Erweiterter Schutz → Schutz vor Verschlüsselung**).

Einstellungen der Komponente "Schutz vor Verschlüsselung"

Einstellung	Beschreibung
Schutz vor Verschlüsselung aktivieren	Dieses Kontrollkästchen aktiviert oder deaktiviert den Schutz von Dateien in lokalen Verzeichnissen, auf die der Netzwerkzugriff über SMB-/NFS-Protokolle möglich ist, vor bösartiger Remote-Verschlüsselung. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Schutzbereiche	Diese Einstellungsgruppe enthält Schaltflächen, mit denen Fenster geöffnet werden können, in denen Sie die Untersuchungsbereiche und die Schutzeinstellungen anpassen können.
Ausschlüsse	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausschlussbereiche** öffnet. In diesem Fenster können Sie eine Liste mit Bereichen festlegen, die von der Untersuchung ausgeschlossen werden sollen.
Ausschlüsse nach Maske	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausschlüsse nach Maske** öffnet. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält den Untersuchungsbereich. Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle einen Untersuchungsbereich, der alle Verzeichnisse des lokalen Dateisystems umfasst.

Einstellungen des Untersuchungsbereichs

Einstellung	Beschreibung
Name des Bereichs	Name des Untersuchungsbereichs
Pfad	Der Pfad zu dem zu untersuchenden Verzeichnis.
Status	Der Status gibt an, ob die App diesen Bereich während ihrer Ausführung untersucht.

Sie können Elemente in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.

Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Liste der Bereiche angeben sind. Um bei Bedarf für das Unterverzeichnis andere Sicherheitseinstellungen festzulegen als für das übergeordnete Verzeichnis, platzieren Sie erforderlichenfalls das Unterverzeichnis in der Liste über dem übergeordneten Verzeichnis.

Fenster "<Neuer Untersuchungsbereich>"

In diesem Fenster können Sie den Schutzbereich der Komponente "Schutz vor Verschlüsselung" hinzufügen und bearbeiten.

Einstellungen des Schutzbereichs

Einstellung	Beschreibung
Name des Bereichs	Eingabefeld für den Namen des Schutzbereichs. Dieser Name wird in der Tabelle im Fenster **Untersuchungsbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung dieses Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, verarbeitet die App diesen Schutzbereich während der Ausführung der Komponente. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die App diesen Schutzbereich während der Ausführung der Komponente nicht. Sie können diesen Bereich zu einem späteren Zeitpunkt zu den Betriebseinstellungen der Komponente hinzufügen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Diese Einstellungsgruppe ermöglicht die Konfiguration des Untersuchungsbereichs. In der Dropdown-Liste der Dateisysteme können Sie den Typ des Dateisystems auswählen: • **Lokal** – Lokale Verzeichnisse. • **Freigegeben** – Ressourcen von Server-Dateisystemen, die über das Samba- oder NFS-Protokoll zugänglich sind. • **Alle freigegebenen** (Standardwert) – Alle Ressourcen des Server-Dateisystems, die über das Samba- oder NFS-Protokoll zugänglich sind.
	Wenn in der Drop-down-Liste der Dateisysteme der Typ **Alle** ausgewählt ist, können Sie rechts in der Drop-down-Liste das Protokoll für den Remote-Zugriff auswählen:

- **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind.
- **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind.

Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Schutzbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie Masken verwenden.

Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben.

Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst.

Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Das Feld darf nicht leer sein.

Masken

Diese Liste enthält die Masken der Objektnamen, die von der App während der Ausführung der Komponente zum Schutz vor Verschlüsselung untersucht werden.

Standardmäßig enthält die Liste die Maske ***** (alle Objekte).

Sie können Masken hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Schutzeinstellungen"

Schutz-Einstellungen

Einstellung	Beschreibung
Aktion beim Erkennen einer Verschlüsselung:	Aktion, die Kaspersky Endpoint Security ausführt, wenn es eine schädliche Verschlüsselung erkennt: • **Informieren** des Benutzers. Kaspersky Endpoint Security blockiert das Gerät, das die Verschlüsselung ausführt nicht. Es protokolliert lediglich ein Ereignis über die Erkennung einer bösartigen Verschlüsselung im Ereignisprotokoll. • **Blockieren** des Geräts, das die Verschlüsselung durchführt (Standardeinstellung).
Nicht vertrauenswürdiges Gerät blockieren für (Min)	In diesem Feld können Sie angeben, wie lange ein nicht vertrauenswürdiges Gerät blockiert werden soll (in Minuten). Wenn der angegebene Zeitpunkt erreicht ist, entfernt die App Kaspersky Endpoint Security nicht vertrauenswürdige Geräte aus der Liste der blockierten Geräte. Sobald das Gerät aus der Liste der nicht vertrauenswürdigen Geräte entfernt wird, hat es wieder Zugriff auf Dateiressourcen im Netzwerk. Wenn ein gefährdetes Gerät blockiert wurde und Sie den Wert dieser Einstellung ändern, ändert sich die Dauer, für die das Gerät blockiert ist, nicht. Diese Dauer ist kein dynamischer Wert und wird zum Zeitpunkt der Blockierung berechnet. Mögliche Werte sind ganze Zahlen zwischen 1 und 4294967295. Standardwert: 30.

Fenster "Ausschlussbereiche"

Die Tabelle enthält Bereiche mit Ausschlüsse von der Untersuchung. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der App angewendet wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "<Neuer Ausschlussbereich>"

In diesem Fenster können Sie einen neuen Bereich mit Untersuchungsausschlüssen hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster Ausschlussbereiche angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss des Bereichs von der Untersuchung während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während ihrer Ausführung von der Untersuchung aus. Wenn das Kontrollkästchen deaktiviert ist, schließt die App diesen Bereich während ihrer Ausführung in die Untersuchung ein. Sie können diesen Bereich zu einem späteren Zeitpunkt ausschließen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Diese Einstellungsgruppe erlaubt die Konfiguration des Ausschlussbereichs. In der Dropdown-Liste der Dateisysteme können Sie den Typ des Dateisystems auswählen, auf dem sich die Verzeichnisse befinden, die von der Untersuchung ausgeschlossen werden sollen: • **Lokal** – Lokale Verzeichnisse. • **Mounted** – Eingebundene Verzeichnisse. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind.
	Wenn in der Drop-down-Liste der Dateisysteme der Typ **Mounted** ausgewählt ist, können Sie rechts in der Drop-down-Liste das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind.

- **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind.

Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Ausschlussbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie Masken und Tags verwenden.

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Sie können auch eine eindeutige Kombination der Tags `[container-id:<Identifikator>]`, `[container-name:<Name>]`, `[image-id:<Identifikator>]` und `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` verwenden.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispiel:

- `[container-name:<Name>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[image-name:<Name>][image-id:<Identifikator>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`
- `[container-name:<Name>][image-id:<Identifikator>][container-id:<Identifikator>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

	Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Als Pfad ist standardmäßig **/** angegeben: Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus.
Name des Dateisystems	Eingabefeld für den Namen des Dateisystems, auf dem sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste auf der rechten Seite das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Untersuchung ausgeschlossen werden. Die Masken werden nur auf Objekte innerhalb des Verzeichnisses angewendet, das im Eingabefeld des Pfades angegeben ist. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen. Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist. Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Maske"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren. Die App untersucht keine Dateien, deren Namen die angegebenen Masken enthalten. Standardmäßig ist die Liste mit Masken leer.

Sie können Masken hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security die ausgewählte Maske für die aus dem Untersuchungsbereich ausgeschlossenen Dateinamen.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens eine Maske ausgewählt ist.

Ein Klick auf die Maske öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien ändern, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Schutz vor Verschlüsselung über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie den Schutz vor Verschlüsselung mithilfe der Aufgabe "Schutz vor Verschlüsselung" (*Anti_Cryptor*) verwalten.

Die Aufgabe zum Schutz vor Verschlüsselung wird standardmäßig nicht gestartet. Sie können diese Aufgabe manuell starten und beenden.

Sie können die Einstellungen für den Schutz vor Verschlüsselung konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zum Schutz vor Verschlüsselung ändern.

Einstellungen für die Aufgabe zum Schutz vor Verschlüsselung

Einstellung	Beschreibung	Werte
ActionOnDetect	Aktiviert die Blockierung nicht vertrauenswürdiger Geräte	`Blockieren` (Standardwert) – Blockierung nicht vertrauenswürdiger Geräte aktivieren. `Informieren` – Blockierung nicht vertrauenswürdiger Geräte deaktivieren.
`BlockTime`	Dauer der Blockierung eines nicht vertrauenswürdigen Geräts in Minuten. Wenn ein betroffener Computer blockiert wurde und Sie den Wert der Einstellung `BlockTime` ändern, ändert sich die Dauer der Blockierung für diesen Computer nicht. Diese Dauer ist kein dynamischer Wert und wird zum Zeitpunkt der Blockierung berechnet.	Ganzzahl von 1 bis 4294967295. Standardwert: 30.
`UseExcludeMasks`	Aktiviert den Ausschluss von Objekten aus dem Schutzbereich, die in der Einstellung `ExcludeMasks.item_#` angegeben sind. Diese Einstellung funktioniert nur, wenn die Einstellung `ExcludeMasks.item_#` angegeben ist.	`Yes` – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, aus dem Schutzbereich ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht aus dem Schutzbereich ausschließen.
`ExcludeMasks.item_#`	Ausschluss von Objekten aus dem Schutzbereich nach Name oder Maske. Mit dieser Einstellung können Sie eine einzelne Datei anhand des Namens oder mehrere Dateien anhand von Masken im Shell-Format aus dem angegebenen Schutzbereich ausschließen. Bevor Sie den Wert dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseExcludeMasks` aktiviert ist. Wenn Sie mehrere Masken angeben möchten, geben Sie jede Maske in einer neuen Zeile mit einem neuen Index an.	Der Standardwert ist nicht angegeben.
Der Abschnitt **[ScanScope.item_ #]** enthält die Bereiche, die von der App geschützt werden sollen. Die Aufgabe zum Schutz vor Verschlüsselung benötigt mindestens einen angegebenen Schutzbereich, der nur in Form allgemeiner Verzeichnisse festgelegt werden kann. Sie können mehrere Abschnitte [ScanScope.item_#] in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge. Der Abschnitt [ScanScope.item_#] enthält folgende Einstellungen:		

`AreaDesc`	Beschreibung des Schutzbereichs mit zusätzlichen Informationen über den Schutzbereich.	Standardwert: `All shared directories`.
`UseScanArea`	Aktiviert den Schutz des angegebenen Bereichs. Um die Aufgabe auszuführen, müssen Sie mindestens einen zu schützenden Bereich angeben.	`Yes` (Standardwert) – Den angegebenen Bereich schützen. `No` – Den angegebenen Bereich nicht schützen
`AreaMask.item_#`	Einschränkungen des Schutzbereichs. Im Schutzbereich schützt die App nur Dateien, die mit Masken im Shell-Format angegeben wurden. Sie können mehrere Elemente vom Typ `AreaMask.item_#` in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge.	Standardwert: * (alle Objekte werden geschützt).
`Path`	Pfad zum Verzeichnis mit den geschützten Objekten.	`<Pfad zum lokalen Verzeichnis>` – schützt eines lokalen Verzeichnisses, dass über SMB oder NFS erreichbar ist. Bei der Angabe des Pfades können Sie Masken verwenden.

		Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. `AllShared` (Standardwert) – Alle über SMB/NFS freigegebenen Ressourcen schützen. `Shared:SMB` – Alle über SMB freigegebenen Ressourcen schützen. `Shared:NFS` – Alle über NFS freigegebenen Ressourcen schützen.
Der Abschnitt **[ExcludedFromScanScope.item_#]** enthält Objekte, die aus allen Abschnitten von [ScanScope.item_#] ausgeschlossen werden müssen. Objekte, die den Regeln eines beliebigen Abschnitts vom Typ [ExcludedFromScanScope.item_#] entsprechen, werden nicht untersucht. Das Format des Abschnitts [ExcludedFromScanScope.item_#] ist dem Format des Abschnitts [ScanScope.item_#] ähnlich. Sie können mehrere Abschnitte [ExcludedFromScanScope.item_#] in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge. Der Abschnitt [ExcludedFromScanScope.item_#] enthält folgende Einstellungen:		
`AreaDesc`	Beschreibung des Ausschlussbereichs vom Schutzbereich mit zusätzlichen Informationen über den Ausschlussbereich.	Standardwert: `All objects`
`UseScanArea`	Schließt den angegebenen Bereich von	`Yes` (Standardwert) – Den

	dem Schutz aus.	angegebenen Bereich vom Schutz ausschließen. `No` – Den angegebenen Bereich nicht vom Schutz ausschließen.
`AreaMask.item_#`	Einschränkung des vom Schutz ausgeschlossenen Bereichs. Im Ausschlussbereich schließt die App nur Objekte aus, die mittels Masken im Shell-Format angegeben wurden. Sie können mehrere Elemente vom Typ `AreaMask.item_#` in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge.	Standardwert: `*` (alle Objekte ausschließen).
`Path`	Pfad zum Verzeichnis mit Objekten, die vom Schutz ausgeschlossen sind.	`<Pfad zum lokalen Verzeichnis>` – Objekte im angegebenen Verzeichnis vom Schutz ausschließen. Bei der Angabe des Pfades können Sie Masken verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

		`Mounted:NFS` – Remote-Verzeichnisse, die auf dem Client-Gerät über das NFS-Protokoll gemountet sind, vom Schutz ausschließen. `Mounted:SMB` – Remote-Verzeichnisse, die auf Client-Gerät über das Samba-Protokoll gemountet sind, vom Schutz ausschließen. `AllRemoteMounted` – Alle Remote-Verzeichnisse, die auf dem Client-Gerät über Samba- oder NFS-Protokolle gemountet sind, vom Schutz ausschließen.

Blockierte Geräte verwalten

Im Rahmen des Schutzes des Geräts vor Netzwerkbedrohungen und bösartiger Remote-Verschlüsselung kann Kaspersky Endpoint Security Remote-Geräte blockieren, deren Aktionen als bösartig eingestuft werden:

- Wenn eine bösartige Verschlüsselung erkannt wird, blockiert die App den Zugriff des Remote-Geräts auf freigegebene Netzwerkverzeichnisse des geschützten Geräts.
- Wenn ein versuchter Netzwerkangriff auf ein geschütztes Gerät erkannt wird, blockiert die App den Netzwerkverkehr vom angreifenden Gerät.

Sie können die Dauer der Blockierung in den Einstellungen zum Schutz vor Netzwerkbedrohungen und Schutz vor bösartiger Remote-Verschlüsselung ändern. Nach Ablauf des angegebenen Zeitraums entsperrt die App das Gerät.

Wenn Sie die App über die Befehlszeile verwalten, können Sie mit den Befehlen zur Verwaltung gesperrter Geräte die Liste der Geräte anzeigen, die aufgrund der Ausführung der App auf dem Gerät gesperrt sind, und diese Geräte manuell entsperren, bevor die Sperrzeit abläuft. Kaspersky Security Center verfügt über keine Tools zur Überwachung und Verwaltung blockierter Geräte, mit Ausnahme der Ereignisse *Netzwerkangriff erkannt* und *Verschlüsselung erkannt*.

-H – Präfix, das angibt, dass der Befehl zur Gruppe der Befehle zur Verwaltung von Geräten gehört, die durch den Schutz vor Verschlüsselung und den Schutz vor Netzwerkbedrohungen gesperrt wurden.

Befehl kesl-control --get-blocked-hosts

Mit diesem Befehl können Sie die Liste der blockierten Geräte in die Konsole ausgeben.

Befehlssyntax

```
kesl-control [-H] --get-blocked-hosts
```

Befehl kesl-control --allow-hosts

Mit diesem Befehl können Sie gesperrte Geräte entsperren.

Befehlssyntax

```
kesl-control [-H] --allow-hosts <Adresse>
```

Argumente und Schlüssel

<Adresse> – IP-Adresse des Geräts oder Subnetzes (IPv4/IPv6, einschließlich Adressen in Kurzform). Sie können mehrere, durch Leerzeichen getrennte IP-Adressen von Geräten oder Subnetzen angeben.

Um die Liste mit blockierten Geräten anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-blocked-hosts
```

Als Ergebnis der Ausführung des Befehls gibt die App die Liste der blockierten Geräte in der Konsole aus.

Um die Blockierung von Geräten aufzuheben, führen Sie den folgenden Befehl aus:

```
kesl-control --allow-hosts <Adresse>
```

Wobei gilt: `<Adresse>` Eine oder mehrere IP-Adressen von Geräten oder Subnetzen (IPv4/IPv6, einschließlich Adresse in Kurzform). Sie können mehrere, durch Leerzeichen getrennte IP-Adressen von Geräten oder Subnetzen angeben.

Als Ergebnis der Ausführung des Befehls entsperrt die App die angegebenen Geräte.

Beispiele:
IPv4-Adressen:

```
dec - 192.168.0.1
dec - 192.168.0.0/24
```

IPv6-Adressen:

```
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210%1
hex - 2001:db8::ae21:ad12
hex - ::ffff:255.255.255.254
hex - ::
```

App-Kontrolle

Mit der Komponente "App-Kontrolle" können Sie den Start von Apps auf geschützten Geräten überwachen. Die App-Kontrolle reduziert das Risiko einer Geräteinfektion, indem der Benutzerzugriff auf Apps eingeschränkt wird.

Um die Komponente nutzen zu können, benötigen Sie eine Lizenz, in der diese Funktionalität enthalten ist.

Diese Funktionalität wird im KESL-Container nicht unterstützt.

Der Start von Apps wird mithilfe der *Regeln der App-Kontrolle* überwacht.

Die Komponente "App-Kontrolle" kann in einem von zwei Modi ausgeführt werden:

- *Deny-Liste*. In diesem Modus erlaubt Kaspersky Endpoint Security allen Benutzern das Starten von allen Apps, mit Ausnahme derer, die in den Regeln der App-Kontrolle angegeben sind. Standardmäßig wird die Komponente "App-Kontrolle" in diesem Modus ausgeführt.
- *Allow-Liste*. In diesem Modus verbietet Kaspersky Endpoint Security allen Benutzern das Starten von allen Apps, mit Ausnahme derer, die in den Regeln der App-Kontrolle angegeben sind.

Wenn die Regeln der App-Kontrolle mit maximaler Genauigkeit erstellt wurden, verbietet Kaspersky Endpoint Security zum einen den Start aller neuen, noch nicht vom Administrator des lokalen Unternehmensnetzwerks überprüften Apps, gewährleistet dabei aber zum anderen die Funktionsfähigkeit des Betriebssystems und der bereits untersuchten Apps, die Benutzer für ihre Arbeit benötigen.

Der Administrator von Kaspersky Security Center oder ein lokaler Benutzer mit in der App zugewiesener Rolle "admin" kann den Start von Prozessen unter dem Root-Konto durch Verwendung der Komponente "App-Kontrolle" verbieten oder erlauben.

Standardmäßig ist die App-Kontrolle deaktiviert. Sie können die App-Kontrolle aktivieren und deaktivieren sowie die Ausführungseinstellungen der Komponente konfigurieren:

- Wählen Sie den Modus der Komponente "App-Kontrolle" aus: *Allow-Liste* oder *Deny-Liste*.
- Erstellen Sie Regeln für die App-Kontrolle für jeden Modus der Komponente.
- Wählen Sie die Aktion aus, die Kaspersky Endpoint Security ausführen soll, wenn ein Versuch erkannt wird, eine App zu starten, die den Regelbedingungen entspricht: *Regeln anwenden* oder *Regeln testen* und über den versuchten Start einer App informieren, die den Regelbedingungen entspricht.

Mit der Aufgabe Inventarisierung können Sie Informationen zu Apps abrufen, die auf geschützten Geräten installiert sind.

Die App-Kontrolle überwacht weder die Ausführung von Skripten aus Interpretern, die nicht von Kaspersky Endpoint Security unterstützt werden, noch die Ausführung von Skripten, die nicht über die Befehlszeile an den Interpreter übergeben werden. Kaspersky Endpoint Security unterstützt die folgenden Interpreter: Python, Perl, Bash, SSH.

Wenn die Regeln für die App-Kontrolle den Start eines Interpreters erlauben, blockiert Kaspersky Endpoint Security keine Skripte, die über diesen Interpreter ausgeführt werden. Wenn die Ausführung von mindestens einem der in der Befehlszeile des Interpreters angegebenen Skripte durch die Regeln für die App-Kontrolle verboten ist, blockiert Kaspersky Endpoint Security alle Skripte, die in der Befehlszeile des Interpreters angegeben sind. Ausnahme: cat script.py | python.

Über die Regeln für die App-Kontrolle

Bei einer *Regel der App-Kontrolle* handelt es sich um eine Reihe von Einstellungen, die die Bedingungen für das Auslösen der Regel und die Aktionen der Komponente "App-Kontrolle" beim Auslösen der Regel enthalten (Benutzern das Starten der App erlauben oder verbieten):

- Zugehörigkeit der App zu den App-Kategorien. Eine *App-Kategorie* ist eine Gruppe von Apps, die über gemeinsame Merkmale verfügen. Darunter fallen z. B. die Kategorie für ausführbare Dateien installierter Apps und die Kategorie für den Standardsatz an notwendigen Apps, die ein Unternehmen in seinem Geschäftsalltag verwendet. Eine Kategorie kann jeweils nur in einer einzigen Regel verwendet werden.

  Die Verwendung der KL-Kategorien von Kaspersky Security Center wird von Kaspersky Endpoint Security nicht unterstützt.

- Das Starten von Apps für ausgewählte Benutzer und/oder Benutzergruppen verbieten oder erlauben. Sie können Benutzer und/oder Benutzergruppen auswählen, denen der Start von Apps aus einer angegebenen Kategorie erlaubt oder verboten werden soll.

- Auslösebedingung für die Regel. Eine Bedingung ist eine Übereinstimmung nach dem Muster "Bedingungstyp – Bedingungskriterium – Bedingungswert". Basierend auf den Bedingungen der Regelauslösung wendet Kaspersky Endpoint Security die Regel auf eine App entweder an oder nicht. Regeln verwenden Einschluss- und Ausschlussbedingungen:

  - *Einschlussbedingungen*. Kaspersky Endpoint Security wendet eine Regel auf eine App an, wenn die App mindestens eine Einschlussbedingung erfüllt.

  - *Ausschlussbedingungen*. Kaspersky Endpoint Security wendet eine Regel nicht auf eine App an, wenn die App mindestens eine Ausschlussbedingung oder keine der Einschlussbedingungen erfüllt.

  Die Bedingungen zum Auslösen der Regel werden anhand der folgenden Kriterien gebildet:

  - Name der ausführbaren App-Datei

  - Name des Verzeichnisses mit der ausführbaren App-Datei

  - Hash der ausführbaren App-Datei Es ist nur SHA256 zulässig.

  Für jedes Kriterium, das in einer Bedingung verwendet wird, muss ein Wert angegeben werden.

  Um Datei- und Verzeichnisnamen anzugeben, können Sie Masken verwenden.

Sie können das Zeichen * (beliebige Zeichenfolge) oder das Zeichen ? (beliebiges einzelnes Zeichen) verwenden, um eine Maske für einen Datei- oder Verzeichnisnamen zu bilden.

Sie können das Zeichen * verwenden, um eine beliebige Anzahl an Zeichen (auch null Zeichen) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/*/file*/` oder `/dir/file*/`.

Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.

Wenn die Einstellungen der ausgeführten App den in der Einschlussbedingung angegebenen Kriterien entsprechen, wird die Regel ausgelöst. In diesem Fall führt Kaspersky Endpoint Security die in der Regel angegebene Aktion aus. Wenn die Einstellungen den in der Ausschlussbedingung angegebenen Kriterien entsprechen, überwacht Kaspersky Endpoint Security den Start der App nicht.

Regeln der App-Kontrolle können einen der folgenden *Ausführungsstatus* haben:

- *Aktiviert* – Die Regel ist aktiviert und Kaspersky Endpoint Security wendet diese Regel während der App-Kontrolle an.
- *Deaktiviert* – Die Regel ist deaktiviert und wird während der App-Kontrolle nicht angewendet.
- *Test* – Kaspersky Endpoint Security erlaubt das Starten von Apps, die den Regelbedingungen entsprechen, registriert aber Informationen über den Start dieser Apps im Bericht.

Der Status der Regel hat eine höhere Priorität als die in der Regel angegebene Aktion.

App-Kontrolle in der Web Console konfigurieren

In der Web Console können Sie Einstellungen der App-Kontrolle in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen** → **Sicherheitskontrolle** → **App-Kontrolle**).

Einstellungen der Komponente "App-Kontrolle"

Einstellung	Beschreibung
App-Kontrolle aktiviert/deaktiviert	Dieser Schalter aktiviert bzw. deaktiviert die App-Kontrolle. Der Schalter ist standardmäßig deaktiviert.
Aktion beim Starten von Anwendungen, die durch Regeln verboten sind	Aktion, die Kaspersky Endpoint Security ausführen soll, wenn ein Versuch erkannt wird, eine App zu starten, welches den festgelegten Regeln entspricht: • **Regeln testen**. Wenn Sie diese Option auswählen, testet Kaspersky Endpoint Security die Regeln und generiert ein Ereignis über den Versuch eine App zu starten, die den Regelbedingungen entspricht. • **Regeln anwenden** (Standardwert). Wenn Sie diese Option auswählen, wendet Kaspersky Endpoint Security die Regeln für die App-Kontrolle an und führt die in den Regeln festgelegte Aktion aus.
Modus der App-Kontrolle	Ausführungsmodus der Komponente zur App-Kontrolle: • **Allow-Liste**. Bei Auswahl dieser Option verbietet Kaspersky Endpoint Security allen Benutzern den Start aller Apps, außer der in den Regeln der App-Kontrolle angegebenen.

	• **Deny-Liste** (Standardwert). Bei Auswahl dieser Option erlaubt Kaspersky Endpoint Security allen Benutzern den Start aller Apps, außer der in den Regeln der App-Kontrolle angegebenen.
Regeln der App-Kontrolle	Der Link **Regeln anpassen** öffnet das Fenster **Regeln für die App-Kontrolle**.
Anwendung von Regeln	In dieser Dropdown-Liste können Sie eine Methode für das Hinzufügen von Regeln festlegen: • **Lokale Regeln durch Regeln aus der Richtlinie ersetzen**. Wenn diese Option ausgewählt ist, werden von der App nur die in der Richtlinie angegebenen Regeln angewendet. • **Regeln aus der Richtlinie zu den lokalen Regeln hinzufügen** (Standardwert) Wenn diese Option ausgewählt ist, werden von der App die Richtlinien, die in den Regeln angegeben wurden, zusammen mit den lokalen Regeln, die auf dem geschützten Gerät konfiguriert sind, angewendet.

Fenster "Regeln der App-Kontrolle"

Die Tabelle **Regeln der App-Kontrolle** enthält Registerkarten mit Regeln für jeden Betriebsmodus der App-Kontrolle: **Deny-Liste (aktiv)** und **Allow-Liste**. Standardmäßig ist die Tabelle mit den Regeln der App-Kontrolle auf beiden Registerkarten leer.

Einstellungen der Regeln der App-Kontrolle

Einstellung	Beschreibung
Kategorie	Der Name der App-Kategorie, die in der Regel verwendet wird.
Status	Der Status der Regel der App-Kontrolle: • *Aktiviert* – Die Regel ist aktiviert und wird während der Ausführung der App-Kontrolle angewendet. • *Deaktiviert* – Die Regel ist deaktiviert und wird während der Ausführung der App-Kontrolle nicht angewendet. • *Test* – Die Aufgabe zur App-Kontrolle erlaubt den Start von Apps, die den Regelbedingungen entsprechen, nimmt aber Informationen über den Start dieser Apps im Bericht auf.

Sie können Regeln der App-Kontrolle hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Fenster "Regel der App-Kontrolle"

In diesem Fenster können Sie die Einstellungen der Regel für die App-Kontrolle anpassen.

Einstellung der Regel für die App-Kontrolle

Einstellung	Beschreibung
Regelbeschreibung	Regelbeschreibung für die App-Kontrolle
Status	Sie können einen Status für die Regel für die App-Kontrolle auswählen: • *Aktiviert* – Die Regel ist aktiviert und wird während der Ausführung der App-Kontrolle angewendet. • *Deaktiviert* – Die Regel ist deaktiviert und wird während der Ausführung der App-Kontrolle nicht angewendet. • *Test* – Die Aufgabe zur App-Kontrolle erlaubt den Start von Apps, die den Regelbedingungen entsprechen, nimmt aber Informationen über den Start dieser Apps im Bericht auf.
Kategorie	Der Link **Kategorie auswählen** öffnet das Fenster **App-Kategorien**.
Benutzer und ihre Rechte	Diese Tabelle enthält eine Liste mit Namen der Benutzer oder Benutzergruppen, für welche die Regel für die App-Kontrolle gilt, sowie die ihnen zugewiesenen Zugriffstypen. Die Tabelle besteht aus den folgenden Spalten: • **Benutzer- oder Gruppenname** – Name des Benutzers oder der Benutzergruppe, für welche die Regel für die App-Kontrolle gilt. • **Zugriff** – Zugriffstyp (Start der App erlauben oder blockieren). Dieser Schalter aktiviert und deaktiviert den Zugriffstyp: **Erlauben** oder **Blockieren** des Starts der App. Sie können Benutzergruppen hinzufügen, anpassen und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Fenster "App-Kategorien"

In diesem Fenster können Sie eine neue Kategorie hinzufügen oder die Einstellungen der Kategorie für die Regel für die App-Kontrolle anpassen.

Die Verwendung der KL-Kategorien von Kaspersky Security Center wird von Kaspersky Endpoint Security nicht unterstützt.

Kategorien der App-Kontrolle

Einstellung	Beschreibung
Kategoriename	Suchzeile für die hinzugefügte App-Kategorie.
Hinzufügen	Durch Klicken auf die Schaltfläche wird der Assistent zum Erstellen einer Kategorie gestartet. Folgen Sie den Anweisungen des Assistenten.
Bearbeiten	Diese Schaltfläche öffnet das Fenster mit den Kategorie-Eigenschaften, in dem Sie die Einstellungen der Kategorie anpassen können.
Löschen	Wenn Sie auf die Schaltfläche klicken, wird die ausgewählte Kategorie gelöscht. Die Kategorie **Goldenes Image (Lokal)** kann nicht gelöscht werden.

Benutzergruppe oder Fenster auswählen

In diesem Fenster können Sie einen lokalen Benutzer oder Domänenbenutzer bzw. eine Gruppe dieser Benutzer angeben, für die Sie eine Regel anpassen möchten.

Einstellung der Regel für die App-Kontrolle

Einstellung	Beschreibung
Manuell	Wenn diese Option ausgewählt ist, müssen Sie im unteren Feld den Namen des lokalen Benutzers oder des Domänenbenutzers oder aber den Namen der Benutzergruppe angeben, auf welche die Regel der App-Kontrolle angewendet wird.
Liste mit Gruppen oder Benutzern	Wenn diese Option ausgewählt ist, können Sie entweder im Suchfeld die Suchkriterien für die Namen der Benutzer oder Benutzergruppen eingeben, auf welche die Regel der App-Kontrolle angewendet wird, oder den Namen der Benutzergruppe aus der unteren Liste auswählen.

App-Kontrolle in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie Einstellungen der App-Kontrolle in den Richtlinieneigenschaften konfigurieren (**Sicherheitskontrolle** → **App-Kontrolle**).

Einstellungen der Komponente "App-Kontrolle"

Einstellung	Beschreibung
App-Kontrolle aktivieren	Dieses Kontrollkästchen aktiviert die Komponente zur App-Kontrolle. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Aktion bei Versuch eines Programmstarts	Aktion, die Kaspersky Endpoint Security ausführen soll, wenn ein Versuch erkannt wird, eine App zu starten, welches den festgelegten Regeln entspricht: • **Regeln anwenden** (Standardwert). Wenn Sie diese Option auswählen, wendet Kaspersky Endpoint Security die Regeln für die App-Kontrolle an und führt die in den Regeln festgelegte Aktion aus. • **Regeln testen**. Wenn Sie diese Option auswählen, testet Kaspersky Endpoint Security die Regeln und generiert ein Ereignis über den Versuch eine App zu starten, die den Regelbedingungen entspricht.
Modus der App-Kontrolle	Ausführungsmodus der Komponente zur App-Kontrolle:

	• **Allow-Liste**. Bei Auswahl dieser Option verbietet Kaspersky Endpoint Security allen Benutzern den Start aller Apps, außer der in den Regeln der App-Kontrolle angegebenen. • **Deny-Liste** (Standardwert). Bei Auswahl dieser Option erlaubt Kaspersky Endpoint Security allen Benutzern den Start aller Apps, außer der in den Regeln der App-Kontrolle angegebenen.
Regeln der App-Kontrolle	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Regeln der App-Kontrolle** öffnet.
Anwendung von Regeln	In dieser Dropdown-Liste können Sie eine Methode für das Hinzufügen von Regeln festlegen: • **Lokale Regeln durch Regeln aus der Richtlinie ersetzen**. Wenn diese Option ausgewählt ist, werden von der App nur die in der Richtlinie angegebenen Regeln angewendet. • **Regeln aus der Richtlinie zu den lokalen Regeln hinzufügen** (Standardwert) Wenn diese Option ausgewählt ist, werden von der App die Richtlinien, die in den Regeln angegeben wurden, zusammen mit den lokalen Regeln, die auf dem geschützten Gerät konfiguriert sind, angewendet.

Fenster "Regeln der App-Kontrolle"

Die Tabelle **Regeln der App-Kontrolle** enthält die Regeln, die von der Komponente zur App-Kontrolle verwendet werden. Standardmäßig ist die Tabelle mit den Regeln der App-Kontrolle leer.

Einstellungen der Regeln der App-Kontrolle

Einstellung	Beschreibung
Kategoriename	Der Name der App-Kategorie, die in der Regel verwendet wird.
Status	Der Status der Regel der App-Kontrolle: • *Aktiviert* – Die Regel ist aktiviert und wird während der Ausführung der App-Kontrolle angewendet. • *Deaktiviert* – Die Regel ist deaktiviert und wird während der Ausführung der App-Kontrolle nicht angewendet. • *Test* – App-Kontrolle erlaubt das Starten von Apps, die den Regelbedingungen entsprechen, registriert aber Informationen über den Start dieser Apps im Bericht. Den Status einer Regel können Sie im Fenster **Regel hinzufügen / Regel ändern** .

Sie können Regeln der App-Kontrolle hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Fenster "Regel hinzufügen"

In diesem Fenster können Sie die Einstellungen der Regel für die App-Kontrolle anpassen.

Regel für die App-Kontrolle hinzufügen

Einstellung	Beschreibung
Beschreibung	Regelbeschreibung für die App-Kontrolle
Regelstatus	In dieser Dropdown-Liste können Sie einen Status für die Regel der App-Kontrolle auswählen: • *Aktiviert* – Die Regel ist aktiviert und wird während der Ausführung der App-Kontrolle angewendet. • *Deaktiviert* – Die Regel ist deaktiviert und wird während der Ausführung der App-Kontrolle nicht angewendet. • *Test* – Die Aufgabe zur App-Kontrolle erlaubt den Start von Apps, die den Regelbedingungen entsprechen, nimmt aber Informationen über den Start dieser Apps im Bericht auf.
Kategorie	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **App-Kategorien** öffnet.
Benutzer und ihre Rechte	Diese Tabelle enthält eine Liste der Benutzer oder Benutzergruppen, für welche die Regel für die App-Kontrolle gilt, sowie die ihnen zugewiesenen Zugriffstypen. Die Tabelle besteht aus den folgenden Spalten: • **Benutzer- oder Gruppenname** – Name des Benutzers oder der Benutzergruppe, für welche die Regel für die App-Kontrolle gilt. • **Zugriff** – Zugriffstyp: Starten der App **erlauben** oder **blockieren**. Sie können Benutzergruppen hinzufügen, anpassen und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Fenster "App-Kategorien"

In diesem Fenster können Sie eine neue Kategorie hinzufügen oder die Einstellungen der Kategorie für die Regel für die App-Kontrolle anpassen.

Die Verwendung der KL-Kategorien von Kaspersky Security Center wird von Kaspersky Endpoint Security nicht unterstützt.

Kategorien der App-Kontrolle

Einstellung	Beschreibung
Kategoriename	Liste der hinzugefügten Kategorien der App-Kontrolle.
Hinzufügen	Durch Klicken auf die Schaltfläche wird der Assistent zum Erstellen einer Kategorie gestartet. Folgen Sie den Anweisungen des Assistenten.
Bearbeiten	Diese Schaltfläche öffnet das Fenster mit den Kategorie-Eigenschaften, in dem Sie die Einstellungen der Kategorie anpassen können.

Fenster "Benutzer oder Gruppe"

In diesem Fenster können Sie einen lokalen Benutzer oder Domänenbenutzer bzw. eine Gruppe dieser Benutzer angeben, für die Sie eine Regel anpassen möchten.

Regel für die App-Kontrolle hinzufügen

Einstellung	Beschreibung
Typ	**Benutzer** oder **Gruppe**, für welchen bzw. welche die Regel gilt.
Benutzer- oder Gruppenname	Name des Benutzers oder der Benutzergruppe, für welche die Regel für die App-Kontrolle gilt.
Zugriff	Zugriffstyp: Starten der App **erlauben** oder **blockieren**.

App-Kontrolle über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die App-Kontrolle mithilfe der vordefinierten Aufgabe "App-Kontrolle" (*Application_Control*) verwalten.

Standardmäßig wird die Aufgabe "App-Kontrolle" nicht ausgeführt. Sie können diese Aufgabe manuell starten und anhalten.

Sie können die Einstellungen der App-Kontrolle auf dem Gerät konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zur App-Kontrolle ändern.

Wenn Sie die Allow-Liste der Apps ändern oder den Start aller Apps und/oder der Apps, die die Ausführung von Kaspersky Endpoint Security beeinflussen, verbieten, müssen Sie für das Ändern der Aufgabeneinstellungen mithilfe einer Konfigurationsdatei oder mithilfe der Befehlszeilenschalter den Befehl `kesl-control --set-settings` mit dem Parameter `--accept` ausführen.

Sie können Einstellungen der App-Kontrolle auch mit den Verwaltungsbefehlen der App-Kontrolle konfigurieren:

- Listen mit Kategorien erstellen und bearbeiten.
- Anzeigen der Listen mit den in der App erstellten Kategorien.
- Regelliste der App-Kontrolle konfigurieren.

Einstellungen der Aufgabe zur App-Kontrolle

Die Tabelle beschreibt alle verfügbaren Werte und Standardwerte aller Einstellungen, die Sie für die Aufgabe zur App-Kontrolle angeben können.

Einstellungen der Aufgabe zur App-Kontrolle

Einstellung	Beschreibung	Werte
`AppControlMode`	Ausführungsmodus der Komponente "App-Kontrolle".	`AllowList` – Kaspersky Endpoint Security verbietet allen Benutzern den Start aller Apps, außer der in den Regeln für die App-Kontrolle angegebenen. `DenyList` (Standardwert) – Kaspersky Endpoint Security erlaubt allen Benutzern den Start aller App, außer der in den Regeln für die App-Kontrolle angegebenen.
`AppControlRulesAction`	Aktion, die Kaspersky Endpoint Security ausführen soll, wenn ein Versuch erkannt wird, eine App zu starten, die den festgelegten Regeln entspricht.	`ApplyRules` (Standardwert) – Kaspersky Endpoint Security wendet die Regeln für die App-Kontrolle an und führt die in den Regeln festgelegte Aktion aus. `TestRules` – Kaspersky Endpoint Security testet die Regeln und generiert ein Ereignis über den Fund einer App gemäß den Regelbedingungen.
Der Abschnitt **[Categories.item_#]** enthält die folgenden Einstellungen:		
`Name`	Der Name der App-Kategorie, für welche die Regel angewendet wird.	
`UseIncludes`	Verwendung von Einschlussbedingungen, um die Regel auszulösen	`Yes` – Regel auf die App anwenden, wenn die App mindestens eine Einschlussbedingung erfüllt. `No` (Standardwert) – Regel nicht auf die App anwenden, selbst wenn die App die Einschlussbedingung erfüllt.
`IncludeFileNames.item_#`	Der Name einer ausführbaren Datei, der die Regel auslöst	Bei der Angabe von Dateinamen können Sie Masken verwenden. Sie können das Zeichen * (beliebige Zeichenfolge) oder das Zeichen ? (beliebiges einzelnes Zeichen) verwenden, um eine Maske für einen Datei- oder Verzeichnisnamen zu bilden. Sie können das Zeichen * verwenden, um eine beliebige Anzahl an Zeichen (auch null Zeichen) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/*/file*/` oder `/dir/file*/`. Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.

`IncludeFolders.item_#`	Der Name eines Verzeichnisses mit einer ausführbaren App-Datei, welche die Regel auslöst	Bei der Angabe von Verzeichnisnamen können Sie Masken verwenden. Sie können das Zeichen * (beliebige Zeichenfolge) oder das Zeichen ? (beliebiges einzelnes Zeichen) verwenden, um eine Maske für einen Datei- oder Verzeichnisnamen zu bilden. Sie können das Zeichen * verwenden, um eine beliebige Anzahl an Zeichen (auch null Zeichen) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/*/file*/` oder `/dir/file*/`. Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.
`IncludeHashes.item_#`	SHA256-Hash einer ausführbaren Datei, der die Regel auslöst	Es ist nur SHA256 zulässig.
`UseExcludes`	Verwendung von Ausschlussbedingungen, um die Regel auszulösen	`Yes` – Regel nicht auf eine App anwenden, wenn die App mindestens eine Ausschlussbedingung oder keine der Einschlussbedingungen erfüllt. `No` (Standardwert) – Regel auf die App anwenden, selbst wenn die App die Ausschlussbedingung erfüllt.
`ExcludeFileNames.item_#`	Der Name einer ausführbaren Datei, der die Regel auslöst	Bei der Angabe von Dateinamen können Sie Masken verwenden. Sie können das Zeichen * (beliebige Zeichenfolge) oder das Zeichen ? (beliebiges einzelnes Zeichen) verwenden, um eine Maske für einen Datei- oder Verzeichnisnamen zu bilden. Sie können das Zeichen * verwenden, um eine beliebige Anzahl an Zeichen (auch null Zeichen) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/*/file*/` oder `/dir/file*/`. Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.

`ExcludeFolders.item_#`	Der Name eines Verzeichnisses mit einer ausführbaren App-Datei, welche die Regel auslöst	Bei der Angabe von Verzeichnisnamen können Sie Masken verwenden. Sie können das Zeichen * (beliebige Zeichenfolge) oder das Zeichen ? (beliebiges einzelnes Zeichen) verwenden, um eine Maske für einen Datei- oder Verzeichnisnamen zu bilden. Sie können das Zeichen * verwenden, um eine beliebige Anzahl an Zeichen (auch null Zeichen) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/*/file*/` oder `/dir/file*/`. Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.
`ExcludeHashes.item_#`	SHA256-Hash einer ausführbaren Datei, der die Regel auslöst	Es ist nur SHA256 zulässig.
Der Abschnitt **[AllowListRules.item_#]** enthält eine Liste mit Regeln für die App-Kontrolle für den Ausführungsmodus *Allow-Liste* (*AllowList*). Jeder Abschnitt [AllowListRules.item_#] enthält folgende Einstellungen:		
`Description`	Regelbeschreibung für die App-Kontrolle	
`AppControlRuleStatus`	Statusvarianten einer Regel der App-Kontrolle:	`On` (Standardwert) – Die Regel ist aktiviert und Kaspersky Endpoint Security wendet diese Regel während der App-Kontrolle an. `Off` – Die Regel wird während der App-Kontrolle nicht angewendet. `Test` – Kaspersky Endpoint Security erlaubt das Starten von Apps, für welche die Regel gilt, erfasst aber Informationen über den Start dieser Apps im Bericht.
`Category`	Der Name der App-Kategorie, für welche die Regel angewendet wird. Als Kategorie kann die Kategorie "Golden Image" angegeben werden.	
Der Abschnitt [**AllowListRules.item_#.ACL.item_#]** listet die Benutzer auf, denen der Start von Apps erlaubt oder verboten ist.		
`Access`	Der Zugriffstyp, der einem Benutzer oder einer Benutzergruppe zugewiesen wird.	`Allow` (Standardwert) – Start der App zulassen. `Block` – Start der App verbieten.

`Principal`	Gibt einen Benutzer oder eine Benutzergruppe an, für welche die Regel für die App-Kontrolle gelten soll.	`\Everyone` (Standardwert) – Die Regel gilt für alle Benutzer. `< Benutzername >` – Name des Benutzers, für den die Regel gilt. `@< Gruppenname >` – Name der Benutzergruppe, für welche die Regel gilt.
Der Abschnitt **[DenyListRules.item_#]** enthält eine Liste mit Regeln für die App-Kontrolle für den Ausführungsmodus *Deny-Liste* (*DenyList*). Jeder Abschnitt [DenyListRules.item_#] enthält die folgenden Einstellungen:		
`Description`	Regelbeschreibung für die App-Kontrolle	
`AppControlRuleStatus`	Statusvarianten einer Regel der App-Kontrolle:	`On` (Standardwert) – Die Regel ist aktiviert und Kaspersky Endpoint Security wendet diese Regel während der App-Kontrolle an. `Off` – Die Regel wird während der App-Kontrolle nicht angewendet. `Test` – Kaspersky Endpoint Security erlaubt das Starten von Apps, für welche die Regel gilt, erfasst aber Informationen über den Start dieser Apps im Bericht.
`Category`	Der Name der erstellten App-Kategorie, für welche die Regel angewendet wird. Als Kategorie kann die Liste der "Golden Image"-Apps angegeben werden.	
Der Abschnitt **[DenyListRules.item_#.ACL.item_#]** listet die Benutzer auf, denen der Start von Apps erlaubt oder verboten ist.		
`Access`	Der Zugriffstyp, der einem Benutzer oder einer Benutzergruppe zugewiesen wird.	`Allow` – Start der App erlauben. `Block` (Standardwert) – Start der App verbieten.
`Principal`	Gibt einen Benutzer oder eine Benutzergruppe an, für welche die Regel für die App-Kontrolle gelten soll.	`\Everyone` (Standardwert) – Die Regel gilt für alle Benutzer. `< Benutzername >` – Name des Benutzers, für den die Regel gilt. `@< Gruppenname >` – Name der Benutzergruppe, für welche die Regel gilt.

Eine Liste mit Kategorien erstellen und bearbeiten

Sie können eine neue Kategorie auf zwei Arten erstellen:

- Unter Verwendung des Befehls "kesl --set-settings" und der Konfigurationsdatei für die Aufgabeneinstellungen der App-Kontrolle (Application_Control)
- Unter Verwendung des Befehls "kesl --set-categories" und der Konfigurationsdatei für die Kategorieeinstellungen.

Um eine Anwendungskategorie zu erstellen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-categories --file <Pfad zur Konfigurationsdatei>
```

Wobei gilt:

`--file <Pfad zur Konfigurationsdatei>` – Pfad der Konfigurationsdatei mit den allgemeinen App-Einstellungen.

Die Datei mit den Kategorieeinstellungen sollte die folgende Struktur haben:

```
[
   {
     "Exclude" : [ "(FilePath like <vollständiger Pfad zur ausführbaren Datei der
    Anwendung>)", "(FileHash == <Hash der ausführbaren Datei>)" ],
     "GUID" : "<eindeutige ID der Kategorie>",
     "Include" : [ "(FilePath like <vollständiger Pfad zur ausführbaren Datei der
    Anwendung>)", "(FileHash == <Hash der ausführbaren Datei>)" ],
     "Name" : "<Kategoriename 1>"
   },
   {
     "Exclude" : [ "(FilePath like <vollständiger Pfad zur ausführbaren Datei der
    Anwendung>)", "(FileHash == <Hash der ausführbaren Datei>)" ],
     "GUID" : "<eindeutige ID der Kategorie>",
     "Include" : [ "(FilePath like <vollständiger Pfad zur ausführbaren Datei der
    Anwendung>)", "(FileHash == <Hash der ausführbaren Datei>)" ],
     "Name" : "<Kategoriename 2>"
   }
]
```

Zur Angabe des Dateinamens in den Feldern `Exclude` und `Include` können Sie Masken verwenden. Der Parameter `Name` ist erforderlich. Wenn Sie den Namen der Kategorie nicht angeben, wird diese nicht erstellt oder wird gelöscht. Der Parameter `GUID` ist ebenfalls erforderlich. Wenn Sie ihn nicht angeben, wird ein Fehler angezeigt und die Kategorie wird nicht erstellt. Der Parameter `GUID` muss ohne Bindestriche angegeben werden.

Sie können das Zeichen * (beliebige Zeichenfolge) oder das Zeichen ? (beliebiges einzelnes Zeichen) verwenden, um eine Maske für einen Datei- oder Verzeichnisnamen zu bilden.

Sie können das Zeichen * verwenden, um eine beliebige Anzahl an Zeichen (auch null Zeichen) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/*/file*/` oder `/dir/file*/`.

Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.

Um eine Liste mit den erstellten App-Kategorien zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-categories [--names <Kategoriename 1> <Kategoriename 2> ...
<Kategoriename N>] --file <Pfad zur Konfigurationsdatei>
```

Wobei gilt:

- `<Kategoriename 1> <Kategoriename 2> ... <Kategoriename N>` – Namen der Kategorien, deren Informationen Sie ändern möchten. Wenn Sie Informationen mehrerer Kategorien ändern möchten, geben Sie die Kategorienamen durch ein Leerzeichen getrennt an. Wenn Sie keinen Kategorienamen angeben, werden vorhandene Kategorien gelöscht und neue Kategorien aus der angegebenen Datei erstellt.

- `--file <Pfad zur Konfigurationsdatei>` – Pfad der Konfigurationsdatei mit den allgemeinen App-Einstellungen.

Eine Liste der erstellten Kategorien anzeigen

Über die Befehlszeile können Sie mithilfe des Befehls zur Verwaltung der App-Kontrolle eine Liste der erstellten App-Kategorien anzeigen.

Die Liste der erstellten Kategorien enthält die folgenden Kategorien:

- Kategorien, die Kaspersky Security Center erstellte wurden.

- Kategorien, die in den Einstellungen der Aufgabe "App-Kontrolle" über die Befehlszeile hinzugefügt wurden

- die Kategorie "GoldenImage", die mithilfe der Aufgabe "Inventarisierung" erstellt wurde (in Kaspersky Security Center oder über die Befehlszeile)

Um eine Liste aller erstellter App-Kategorien anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-categories --file <Pfad zur Konfigurationsdatei> [--json]
```

Wobei gilt:

- `--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei im JSON-Format, in der die Einstellungen ausgegeben werden.

- `--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie das Argument "--json" nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Kaspersky Endpoint Security zeigt folgende Informationen zu jeder App-Kategorie an:

- die eindeutige ID (GUID) der Kategorie

- Name der Kategorie

- Liste der Einschlussbedingungen, um die Regel auszulösen

- Liste der Ausschlussbedingungen, um die Regel auszulösen

Um eine Liste mit den erstellten App-Kategorien anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-categories [--names <Kategoriename 1> <Kategoriename 2> ...
<Kategoriename N>] --file [<Pfad zur Konfigurationsdatei>] [--json]
```

Wobei gilt:

- `<Kategoriename 1> <Kategoriename 2> ... <Kategoriename N>` – Namen der Kategorien, deren Informationen Sie anzeigen möchten. Wenn Sie Informationen mehrerer Kategorien anzeigen möchten, geben Sie die Kategorienamen durch ein Leerzeichen getrennt an.

- `--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei im JSON-Format, in der Liste der Kategorien ausgegeben wird.

- `--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie das Argument "--json" nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Wenn Sie in den Einstellungen der Aufgabe zur App-Kontrolle im Abschnitt `[Categories.item_#]` zum Einschließen oder Ausschließen von Bedingungen für das Auslösen einer Regel symbolische Links zur App-Datei oder zu einem Verzeichnis mit einer ausführbaren Datei angegeben haben, dann wird beim Anzeigen der Liste der App-Kategorien für diese Bedingungen der Quellpfad angezeigt, auf den der symbolische Link verweist.

Einstellung der Liste mit Regeln für die App-Kontrolle

Um eine Liste mit den Regeln der App-Kontrolle anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 21 [--file <Pfad zur Konfigurationsdatei>] [--json]
```

Wobei gilt:

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, in der die Einstellungen ausgegeben werden.

`--json` – Gibt Daten im JSON-Format aus.

Kaspersky Endpoint Security zeigt folgende Informationen zu Regeln der App-Kontrolle an:

- Ausführungsmodus der Komponente zur App-Kontrolle

- Aktion, die von der App-Kontrolle ausgeführt wird, wenn ein Versuch erkannt wird, eine Anwendung zu starten, die der konfigurierten Regel entspricht

- Beschreibung der Regel der App-Kontrolle (falls vorhanden)

- Ausführungsstatus der Regel der App-Kontrolle

- Name der App-Kategorie, für welche die Regel angewendet wird

- Zugriffstyp, der dem Benutzer oder der Benutzergruppe zugewiesen ist

- Benutzer oder Benutzergruppe, für welche die Regel der App-Kontrolle zutrifft

Um die Liste mit den App-Kategorien und den Regeln der App-Kontrolle zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 21 [--file <Pfad zur Konfigurationsdatei>] [--json]
```

Wobei gilt:

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die Einstellungen importiert werden.

`--json` – Importiert die Daten aus einer Datei im JSON-Format importiert.

Um die Liste mit den App-Kategorien und den Regeln der App-Kontrolle zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 21 --set-to-default
```

Inventarisierung

Mithilfe der Inventarisierungsaufgabe erhalten Sie Informationen über alle ausführbaren Dateien der App, die auf den Client-Geräten gespeichert sind. Das Abrufen von Informationen über die Apps, die auf den Geräten installiert sind, kann sinnvoll sein, um z. B. Regeln für die App-Kontrolle zu erstellen.

Diese Funktionalität wird im KESL-Container nicht unterstützt.

Um die Aufgabe nutzen zu können, benötigen Sie eine Lizenz, in der diese Funktionalität enthalten ist.

Sie können die folgenden Einstellungen der Inventarisierung konfigurieren:

- Wählen Sie die Objekttypen aus, die die App während der Inventarisierung auf dem Gerät erkennen soll (Dateien, Skripte).
- Aktivieren oder deaktivieren Sie das Hinzufügen von Apps, die von der Aufgabe "Inventarisierung" auf dem Gerät erkannt wurden, zur App-Kategorie "Golden Image".
- Konfigurieren Sie Inventarisierungsbereiche (Pfade zu Verzeichnissen, in denen nach ausführbaren App-Dateien gesucht werden soll).
- Konfigurieren Sie Ausschlüsse von der Inventarisierung.

Inventarisierung in der Web Console

In der Web Console können Sie mithilfe der Aufgabe *Inventarisierung* eine Inventarisierung der Apps auf einem geschützten Gerät durchführen.

Sie können Benutzeraufgaben für die Inventarisierung erstellen und ausführen. Sie können die Inventarisierungseinstellungen konfigurieren, indem Sie die Einstellungen für diese Aufgaben ändern.

In der Datenbank der App Kaspersky Security Center können Informationen über 150.000 verarbeitete Dateien gespeichert werden. Wenn diese Anzahl von Datensätzen erreicht ist, werden keine neuen Dateien verarbeitet. Damit die Aufgabe zur Inventarisierung wieder ausgeführt werden kann, müssen Sie von dem Gerät mit installiertem Kaspersky Endpoint Security die Dateien löschen, die infolge einer früheren Inventarisierung in der Datenbank von Kaspersky Security Center erfasst wurden.

Einstellungen der Inventarisierungsaufgabe

Einstellung	Beschreibung
Dateien zur Goldenen Kategorie hinzufügen	Das Kontrollkästchen aktiviert oder deaktiviert das Hinzufügen von Anwendungen, die von der Inventarisierungsaufgabe auf dem Gerät erkannt wurden, zur App-Kategorie "Goldenen Kategorie" (Golden Image). Wenn das Kontrollkästchen aktiviert ist, können Sie die Kategorie "Golden Image" in den Regeln für die App-Kontrolle verwenden. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Alle ausführbaren Dateien untersuchen	Das Kontrollkästchen aktiviert und deaktiviert die Untersuchung von ausführbaren Dateien. Das Kontrollkästchen ist standardmäßig aktiviert.

Binärdateien untersuchen	Das Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Binärdateien (mit den Erweiterungen elf, java und pyc). Das Kontrollkästchen ist standardmäßig aktiviert.
Skripte untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Skripten. Das Kontrollkästchen ist standardmäßig aktiviert.
Bereiche der Inventarisierung	Eine Tabelle mit Inventarisierungsbereichen, die von der App untersucht werden sollen. Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle einen einzigen Inventarisierungsbereich: /usr/bin. Sie können Inventarisierungsbereiche in der Tabelle hinzufügen, konfigurieren, löschen, nach oben verschieben und nach unten verschieben. Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten. Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren. Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde. Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben. Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren. Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde. Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist. Ein Klick auf den Namen des Untersuchungsbereichs öffnet das Fenster **<Name des Untersuchungsbereichs>**. In diesem Fenster können Sie die Einstellungen des ausgewählten Untersuchungsbereichs ändern. Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **<Neuer Untersuchungsbereich>**. In diesem Fenster können Sie einen neuen Untersuchungsbereich festlegen.

Fenster zum Hinzufügen des Untersuchungsbereichs

In diesem Fenster können Sie einen Untersuchungsbereich für die Inventarisierungsaufgabe hinzufügen und bearbeiten.

Einstellungen des Inventarisierungsbereichs

Einstellung	Beschreibung
Name des Bereichs	Eingabefeld für den Namen des Inventarisierungsbereichs. Dieser Name wird in der Tabelle im Abschnitt **Untersuchungseinstellungen** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung des Bereichs während der Ausführung der Aufgabe. Wenn das Kontrollkästchen aktiviert ist, verarbeitet die App diesen Inventarisierungsbereich während der Ausführung der Aufgabe. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die App diesen Inventarisierungsbereich während der Ausführung der Aufgabe nicht. Im Folgenden können Sie diesen Bereich zu den Aufgabeneinstellungen hinzufügen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Eingabefeld für den Pfad des lokalen Verzeichnisses, das in den Inventarisierungsbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld darf nicht leer sein. Standardmäßige Pfadangabe **/** – Die App untersucht alle Verzeichnisse des lokalen Dateisystems.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der App während der Ausführung der Aufgabe untersucht werden. Standardmäßig enthält die Liste die Maske ***** (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Abschnitt "Ausschlussbereiche"

Im Abschnitt **Ausschlussbereiche** können Sie für die Inventarisierungsaufgabe Ausschlussbereiche für die Untersuchung konfigurieren.

Fenster "Ausschlussbereiche"

Die Tabelle enthält Bereiche mit Ausschlüsse von der Untersuchung. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der App angewendet wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster zum Hinzufügen des Ausschlussbereichs

In diesem Fenster können Sie einen Bereich mit Untersuchungsausschlüssen für die Inventarisierungsaufgabe hinzufügen und bearbeiten.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster **Ausschlussbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss des Bereichs während der Ausführung der Aufgabe. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während ihrer Ausführung aus. Wenn das Kontrollkästchen deaktiviert ist, schließt die App diesen Bereich während ihrer Ausführung ein. Im Folgenden können Sie diesen Bereich aus der Untersuchung ausnehmen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Eingabefeld für den Pfad des lokalen Verzeichnisses, das in den Bereich mit Ausschlüsse von der Inventarisierung aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld darf nicht leer sein.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Untersuchung ausgeschlossen werden. Sie können Masken hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Inventarisierung in der Verwaltungskonsole

In der Verwaltungskonsole von Kaspersky Security Center können Sie mithilfe der Aufgabe *Inventarisierung* eine Inventarisierung der Apps auf einem geschützten Gerät durchführen.

Sie können Benutzeraufgaben für die Inventarisierung erstellen und ausführen. Sie können die Untersuchungseinstellungen konfigurieren, indem Sie die Aufgabeneinstellungen ändern.

In der Datenbank der App Kaspersky Security Center können Informationen über 150.000 verarbeitete Dateien gespeichert werden. Wenn diese Anzahl von Datensätzen erreicht ist, werden keine neuen Dateien verarbeitet. Damit die Aufgabe zur Inventarisierung wieder ausgeführt werden kann, müssen Sie von dem Gerät mit installiertem Kaspersky Endpoint Security die Dateien löschen, die infolge einer früheren Inventarisierung in der Datenbank von Kaspersky Security Center erfasst wurden.

Einstellungen der Inventarisierungsaufgabe

Einstellung	Beschreibung
Dateien zur Goldenen Kategorie hinzufügen	Das Kontrollkästchen aktiviert oder deaktiviert das Hinzufügen von Anwendungen, die von der Inventarisierungsaufgabe auf dem Gerät erkannt wurden, zur App-Kategorie "Goldenen Kategorie" (Golden Image). Wenn das Kontrollkästchen aktiviert ist, können Sie die Kategorie "Golden Image" in den Regeln für die App-Kontrolle verwenden. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Alle ausführbaren Dateien untersuchen	Das Kontrollkästchen aktiviert und deaktiviert die Untersuchung von ausführbaren Dateien. Das Kontrollkästchen ist standardmäßig aktiviert.
Binärdateien untersuchen	Das Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Binärdateien (mit den Erweiterungen elf, java und pyc). Das Kontrollkästchen ist standardmäßig aktiviert.
Skripte untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Skripten. Das Kontrollkästchen ist standardmäßig aktiviert.
Bereiche der Inventarisierung	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster Untersuchungsbereiche öffnet.

Im Abschnitt **Ausschlussbereiche** für die Inventarisierungsaufgabe können Sie auch Ausschlussbereiche für die Untersuchung konfigurieren.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält den Untersuchungsbereich. Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle einen einzigen Untersuchungsbereich: /usr/bin.

Einstellungen des Untersuchungsbereichs der Inventarisierungsaufgabe

Einstellung	Beschreibung
Name des Bereichs	Name des Untersuchungsbereichs
Pfad	Der Pfad zu dem zu untersuchenden Verzeichnis.
Status	Der Status gibt an, ob die App diesen Bereich während ihrer Ausführung untersucht.

Sie können Elemente in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.

Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Liste der Bereiche angeben sind. Um bei Bedarf für das Unterverzeichnis andere Sicherheitseinstellungen festzulegen als für das übergeordnete Verzeichnis, platzieren Sie erforderlichenfalls das Unterverzeichnis in der Liste über dem übergeordneten Verzeichnis.

Fenster "<Neuer Untersuchungsbereich>"

In diesem Fenster können Sie einen Untersuchungsbereich für die Inventarisierungsaufgabe hinzufügen und bearbeiten.

Einstellungen des Inventarisierungsbereichs

Einstellung	Beschreibung
Name des Untersuchungsbereichs	Eingabefeld für den Namen der Untersuchungsbereichs. Dieser Name wird in der Tabelle im Fenster **Untersuchungsbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung des Bereichs während der Ausführung der Aufgabe. Wenn das Kontrollkästchen aktiviert ist, verarbeitet die App diesen Untersuchungsbereich während der Ausführung der Aufgabe. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die App diesen Untersuchungsbereich während der Ausführung der Aufgabe nicht. Im Folgenden können Sie diesen Bereich zu den Aufgabeneinstellungen hinzufügen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Eingabefeld für den Pfad des lokalen Verzeichnisses, das in den Untersuchungsbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld darf nicht leer sein.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der App während der Ausführung der Aufgabe untersucht werden. Standardmäßig enthält die Liste die Maske * (alle Objekte).

Sie können Masken hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Abschnitt "Ausschlüsse"

Einstellungen der Ausschlüsse von der Untersuchung

Einstellungsgruppe	Beschreibung
Ausschlussbereiche	Diese Parametergruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster Ausschlussbereiche öffnet. In diesem Fenster können Sie eine Liste mit Bereichen festlegen, die von der Überwachung ausgeschlossen werden sollen.

Fenster "Ausschlussbereiche"

Die Tabelle enthält Bereiche mit Ausschlüsse von der Untersuchung. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der App angewendet wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "<Neuer Ausschlussbereich>"

In diesem Fenster können Sie einen Bereich mit Untersuchungsausschlüssen für die Inventarisierungsaufgabe hinzufügen und bearbeiten.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster **Ausschlussbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss des Bereichs während der Ausführung der Aufgabe. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während ihrer Ausführung aus. Wenn das Kontrollkästchen deaktiviert ist, schließt die App diesen Bereich während ihrer Ausführung ein. Im Folgenden können Sie diesen Bereich aus der Untersuchung ausnehmen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Eingabefeld für den Pfad des lokalen Verzeichnisses, das in den Bereich mit Ausschlüsse von der Inventarisierung aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken verwenden. Das Feld darf nicht leer sein. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Untersuchung ausgeschlossen werden.

Sie können Masken hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Inventarisierung über die Befehlszeile

Über die Befehlszeile können Sie eine Inventarisierung der Apps auf dem geschützten Gerät auf folgende Arten durchführen:

- Mithilfe der vordefinierten Aufgabe Inventarisierung (*Inventory_Scan*). Sie können diese Aufgabe manuell starten und beenden und den Zeitplan für den Aufgabenstart konfigurieren. Sie können die Einstellungen für die Untersuchung konfigurieren, indem Sie die Einstellungen für diese Aufgabe ändern.
- Mithilfe von Benutzeraufgaben für die Inventarisierung (Aufgaben vom Typ *InventoryScan*). Sie können Benutzeraufgaben manuell starten, beenden, anhalten und fortsetzen und den Zeitplan für den Aufgabenstart konfigurieren.

Sie können die Liste der Apps, die auf einem Gerät als Ergebnis der Ausführung der Inventarisierungsaufgabe erkannt wurden, mithilfe der Befehle zur Verwaltung der App-Kontrolle anzeigen.

Einstellungen der Inventarisierungsaufgabe

Die Tabelle beschreibt alle verfügbaren Werte und Standardwerte aller Einstellungen, die Sie für die Inventarisierungsaufgabe angeben können.

Einstellungen der Inventarisierungsaufgabe

Einstellung	Beschreibung	Werte
`ScanScripts`	Aktiviert die Untersuchung von Skripten.	`Yes` (Standardwert) – Skripte untersuchen. `No` – Skripte nicht untersuchen.
`ScanBinaries`	Aktiviert die Untersuchung von Binärdateien (elf, java und pyc).	`Yes` (Standardwert) – Binärdateien untersuchen. `No` – Binärdateien nicht untersuchen.
`ScanAllExecutable`	Aktiviert die Untersuchung von Dateien mit Executable Bit.	`Yes` (Standardwert) – Dateien mit Executable Bit untersuchen. `No` – Dateien mit Executable Bit nicht untersuchen.
`CreateGoldenImage`	Anwendungen, die von der Inventarisierungsaufgabe auf dem Gerät gefunden wurden, zur App-Kategorie "Golden Image" hinzufügen. Wenn die Einstellung `CreateGoldenImage=Yes` festgelegt ist, können Sie in den Regeln der App-Kontrolle die App-Kategorie "Golden Image" verwenden.	`Yes` – Erkannte Anwendungen zur App-Kategorie "Golden Image" hinzufügen. `No` (Standardwert) – Erkannte Anwendungen nicht zur App-Kategorie "Golden Image" hinzufügen.
Der Abschnitt **[ScanScope.item_#]** enthält die folgenden Parameter:		
`AreaDesc`	Beschreibung des Inventarisierungsbereichs mit zusätzlichen Informationen Inventarisierungsbereich. Die maximale Länge einer Zeichenfolge, die mit dieser Einstellung angegeben werden kann, beträgt 4096 Zeichen.	Standardwert: `All objects`.
`UseScanArea`	Aktiviert die Untersuchung des angegebenen Inventarisierungsbereichs. Um die Aufgabe auszuführen, müssen Sie mindestens einen Inventarisierungsbereich angeben.	`Yes` (Standardwert) – Den angegebenen Inventarisierungsbereich untersuchen. `No` – Den angegebenen Inventarisierungsbereich nicht untersuchen.
`AreaMask.item_#`	Einschränkung des Inventarisierungsbereichs. Im Inventarisierungsbereich untersucht die App nur Dateien, die mittels Masken im Shell-Format angegeben wurden. Wenn die Einstellung nicht angegeben wurde, untersucht die App alle Objekte im Inventarisierungsbereich. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: * (alle Objekte untersuchen)
`Path`	Pfad zum Verzeichnis mit untersuchten Objekten.	`<Pfad zum lokalen Verzeichnis>` – Objekte im angegebenen Verzeichnis untersuchen. Der Standardwert ist `/usr/bin`
Der Abschnitt **[ExcludedFromScanScope.item_#]** enthält folgende Einstellungen:		
`AreaDesc`	Beschreibung des Ausschlussbereichs von der Inventarisierung mit zusätzlicher	Der Standardwert ist nicht angegeben.

	Information über den Inventarisierungsbereich	
`UseScanArea`	Schließt den angegebenen Bereich von der Inventarisierung aus.	`Yes` (Standardwert) – Den angegebenen Bereich ausschließen. `No` – Den angegebenen Bereich nicht ausschließen.
`AreaMask.item_#`	Einschränkung des Ausschlussbereichs der Inventarisierung mittels Masken im Shell-Format. Wenn die Einstellung nicht angegeben wurde, schließt die App alle Objekte im Inventarisierungsbereich aus. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: `*` (alle Objekte ausschließen)
`Path`	Pfad zum Verzeichnis mit ausgeschlossenen Objekten.	`<Pfad zum lokalen Verzeichnis>` – Objekte im angegebenen Verzeichnis von der Untersuchung ausschließen. Bei der Angabe des Pfades können Sie Masken verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Liste der gefundenen Apps anzeigen

Um die Liste der auf dem Gerät gefundenen Apps anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-app-list [--json]
```

Wobei gilt: `--json` – Gibt Daten im JSON-Format aus.

Kaspersky Endpoint Security zeigt für gefundene Apps die folgenden Informationen an:

- **Datum und Uhrzeit der Inventarisierung**. Datum und Uhrzeit der Ausführung der Inventarisierungsaufgabe.
- **Anzahl der Apps**. Anzahl der auf dem Gerät gefundenen Apps.
- Liste der Apps mit folgenden Informationen:
  - **Pfad**. Pfad zur App.
  - **Hash**. Hash-Summe der App.
  - **Typ**. Typ der App. Zum Beispiel: `Script`, `Executable`.
  - **Kategorie**. Kategorien, zu denen die App gehört (falls sie zuvor erstellt wurden). Sie können die Liste der erstellten App-Kategorien mit dem Befehl `kesl-control --get-categories` anzeigen.

Wenn Sie eine neue Kategorie hinzufügen, werden deren Informationen in der Liste der Apps nicht automatisch aktualisiert. Um die Liste der Apps zu aktualisieren, müssen Sie die Inventarisierungsaufgabe neu starten.

Gerätekontrolle

Mit der Komponente *Gerätekontrolle* können Sie den Benutzerzugriff auf zusätzliche oder externe Geräte verwalten, die auf dem Client-Gerät installiert oder daran angeschlossen sind (z. B. Festplatten, Kameras oder WLAN-Module). Durch die Zugriffskontrolle können Sie das Client-Gerät vor einer Infektion schützen, wenn Sie externe Geräte anschließen, und Datenverlust oder Datenlecks verhindern.

Diese Funktionalität wird im KESL-Container nicht unterstützt.

Die Komponente "Gerätekontrolle" wird beim Start von Kaspersky Endpoint Security automatisch mit den Standardeinstellungen aktiviert.

Die Gerätekontrolle verwaltet den Zugriff auf den folgenden Ebenen:

- **Gerätetyp** gemäß der Klassifizierung der Komponente "Gerätekontrolle" (z. B. Drucker, Wechseldatenträger, CD-/DVD-Laufwerke). Für jeden Gerätetyp kann einer der folgenden Zugriffsmodi verwendet werden:
  - *Erlauben* – Gewährt Zugriff auf Geräte dieses Typs.
  - *Blockieren* – Blockiert den Zugriff auf Geräte dieses Typs.
  - *Je nach Bus-Verbindung* – Erlaubt oder blockiert den Zugriff auf Geräte, abhängig vom Zugriffsmodus für den Bus, über den das Gerät verbunden ist.
  - *Nach Regeln* – Zugriff auf Geräte erlauben oder blockieren, abhängig von den Regeln für den Zugriff auf Geräte. *Gerätezugriffsregel* – Eine Reihe von Einstellungen, die bestimmen, welche Benutzer zu welcher Zeit auf Geräte zugreifen können, die auf dem Client-Gerät installiert oder daran angeschlossen sind.

    Wenn ein Gerät, auf das der Zugriff verboten ist, angeschlossen wird, verweigert die App den in der Regel angegebenen Benutzern den Zugriff auf dieses Gerät und zeigt eine Benachrichtigung an. Beim Versuch, auf diesem Gerät zu lesen und zu schreiben, verweigert die App den in der Regel angegebenen Benutzern das Lesen und Schreiben, ohne eine Benachrichtigung anzuzeigen.

    Wenn Sie versuchen, eine Aktion auf einem Gerät mit festgelegtem Zugriffsmodus *Nach Regeln* auszuführen, zum Zeitpunkt des Zugriffs aber keine Regel aktiv ist, wird die Aktion mit dem Gerät verboten.
- **Bus-Verbindung**. *Bus-Verbindung* – Schnittstelle, über die Geräte mit dem Client-Gerät verbunden werden (z. B. USB, FireWire). Für Bus-Verbindungen kann einer der folgenden Zugriffsmodi verwendet werden:
  - *Erlauben* – Gewährt Zugriff auf Geräte, die über diese Bus-Verbindung verbunden sind.
  - *Blockieren* – Blockiert den Zugriff auf Geräte, die über diese Bus-Verbindung verbunden sind.

  Beispielsweise kann der Zugriff auf alle über USB angeschlossenen Geräte verweigert werden.

Standardmäßig ist für alle Gerätetypen der Zugriffsmodus *Je nach Bus-Verbindung* und für Bus-Verbindungen der Zugriffsmodus *Erlauben* ausgewählt. Basierend auf diesen Einstellungen gewährt die Gerätekontrolle Benutzern vollen Zugriff auf alle Geräte.

Das Blockieren von Geräten nach Gerätetyp und Verbindungsbus über den Systemgerätetreiber wird von den Linux-Kerneln 3.10, 5.14, 5.15, 5.17, 6.1 nicht unterstützt. Mit diesen Kernels und im Zugriffsmodus *Nach Regeln* wird nur das Öffnen von Dateien und das Lesen von Verzeichnissen (d. h. das Abrufen von Datei- und Verzeichnisnamen) blockiert. Auf Systemen, welche die Fanotify-Technologie nicht unterstützen, wird das Blockieren von Lesen von Verzeichnisse nicht unterstützt.

Wenn die Komponente "Gerätekontrolle" zum ersten Mal gestartet wird, wird das Ereignis *Zugriff auf Gerät erlaubt* für alle erkannten Geräte mit einem bekannten Geräte- oder Bustyp generiert. Bei nachfolgenden Starts werden keine wiederholten Ereignisse für diese Geräte generiert, sofern für diese Geräte keine Änderungen an den Kontrolleinstellungen vorgenommen wurden.

Wenn die Komponente "Gerätekontrolle" beendet wird, entsperrt die App den Zugriff auf gesperrte Geräte.

Sie können die Gerätekontrolle aktivieren und deaktivieren sowie die folgenden Ausführungseinstellungen der Komponente konfigurieren:

- Auswählen des Ausführungsmodus der App, beim Versuch, auf ein Gerät zuzugreifen, auf das der Zugriff gemäß den Einstellungen der Gerätekontrolle verboten ist: Blockieren oder nur über einen Zugriffsversuch auf das Gerät informieren.
- Auswählen des Zugriffsmodus für Geräte je nach ihrem Typ.
- Auswählen des Zugriffsmodus für den Bus, über den Geräte verbunden werden.
- Ausschließen einzelner Geräte aus dem Aktionsbereich der Gerätekontrolle, indem Sie diese zur Liste der vertrauenswürdigen Geräte hinzufügen. *Vertrauenswürdige Geräte* – Geräte, auf die Benutzer vollen Zugriff haben. Sie können Geräte nach ID oder Geräte-ID-Maske zur Liste der vertrauenswürdigen Geräte hinzufügen. Sie können beispielsweise den Zugriff auf bestimmte USB-Geräte oder nur auf USB-Laufwerke zuzulassen. In der Folge wird der Zugriff auf andere USB-Geräte verweigert.

  Wenn Sie die App über die Befehlszeile steuern, können Sie die IDs der verbundenen Geräte anzeigen, indem Sie den Befehl `kesl-control --get-device-list` auf dem Client-Gerät ausführen.

  Wenn Sie eine App mithilfe von Kaspersky Security Center verwalten, können Informationen über Geräte, die auf Client-Geräten installiert oder mit ihnen verbunden sind, an den Administrationsserver übertragen werden. Die Informationsübertragung ist standardmäßig aktiviert.

  > Informationen zu Geräten werden nur übertragen, wenn ein Client-Gerät durch eine aktive Richtlinie verwaltet wird und eine Synchronisierung mit dem Administrationsagenten stattgefunden hat (wird in dem Intervall ausgeführt, das in den Eigenschaften der Richtlinie des Administrationsagenten festgelegt ist – standardmäßig alle 15 Minuten).

- Sie können den Zeitplan für den Gerätezugriff konfigurieren (nur für Festplatten, Wechseldatenträger, Disketten und CD-/DVD-Laufwerke).

  > Wenn in den allgemeinen Einstellungen der App des Blockieren des Zugriffs auf Dateien während der Untersuchung deaktiviert ist, kann der Zugriff auf Geräte mithilfe des Zugriffszeitplans für Geräte nicht blockiert werden.

- Konfigurieren Sie Zugriffsregeln für Geräte je nach ihrem Typ. Sie können bestimmten Benutzern zu bestimmten Zeiten den Zugriff erlauben oder verweigern.

> Die Gerätekontrolle ignoriert Ausschlüsse von Mountpunkten. Der Zugriff auf ein Gerät, das an einem ausgeschlossenen Punkt gemountet ist, kann gemäß den konfigurierten Einstellungen der Gerätekontrolle eingeschränkt werden.

Gerätekontrolle in der Web Console konfigurieren

In der Web Console können Sie Einstellungen der Gerätekontrolle in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen → Sicherheitskontrolle → Gerätekontrolle**).

Einstellungen der Komponente "Gerätekontrolle"

Einstellung	Beschreibung
Gerätekontrolle aktiviert/deaktiviert	Dieser Schalter aktiviert bzw. deaktiviert die Gerätekontrolle. Der Schalter ist standardmäßig aktiviert.
Vertrauenswürdige Geräte konfigurieren	Dieser Link öffnet das Fenster **Vertrauenswürdige Geräte**. In diesem Fenster können Sie Geräte zu einer Liste nach ID vertrauenswürdiger Geräte oder durch Auswahl aus einer Liste der auf dem Gerät gefundenen Geräte hinzufügen.
Ausführungsmodus der Gerätekontrolle	Ausführungsmodus der App beim Zugriffsversuch auf ein Gerät, auf das der Zugriff gemäß den Einstellungen der Gerätekontrolle verboten ist. • **Informieren**. Wenn Sie diese Option auswählen, testet Kaspersky Endpoint Security den ausgewählten Zugriffsmodus und generiert ein Ereignis über den Fund eines Zugriffsversuchs auf das Gerät. • **Blockieren** (Standardwert). Wenn Sie diese Option auswählen, wendet Kaspersky Endpoint Security den für das Gerät oder den Bus angegebenen Zugriffsmodus an.
Einstellungen für Zugriffe nach Gerätetypen konfigurieren	Dieser Link öffnet das Fenster **Gerätetypen**. In diesem Fenster können Sie Zugriffseinstellungen für Geräte je nach ihrem Typ konfigurieren.
Einstellungen für Zugriffe nach Bus-Verbindungen konfigurieren	Dieser Link öffnet das Fenster **Bus-Verbindungen**. In diesem Fenster können Sie Zugriffseinstellungen für Bus-Verbindungen konfigurieren.

Fenster "Vertrauenswürdige Geräte"

Die Tabelle enthält eine Liste der vertrauenswürdigen Geräte. Standardmäßig die Tabelle leer.

Einstellungen eines vertrauenswürdigen Geräts

Einstellung	Beschreibung
Geräte-ID	ID eines vertrauenswürdigen Geräts.
Gerätename	Name eines vertrauenswürdigen Geräts.
Gerätetyp	Typ eines vertrauenswürdigen Geräts (z. B. Festplatte oder Smartcard-Leser).
Name des Client-Geräts	Name des Client-Geräts, mit dem das vertrauenswürdige Gerät verbunden ist.
Kommentar	Kommentar zu einem vertrauenswürdigen Gerät.

Sie können ein Gerät zu einer Liste vertrauenswürdiger Geräte nach Geräte-ID oder durch Auswahl des gewünschten Geräts aus einer Liste der auf dem Benutzergerät gefundenen Geräte hinzufügen.

Sie können vertrauenswürdige Geräte in der Tabelle bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Sie können auch eine Liste von Geräten aus einer Datei importieren, indem Sie auf die Schaltfläche **Importieren** klicken und die Liste der hinzugefügten Geräte über die Schaltflächen **Exportieren** in eine Datei exportieren. Beim Importieren wird Ihnen vorgeschlagen, entweder die Liste der vertrauenswürdigen Geräte zu ersetzen oder die Geräte zu einer bestehenden Liste hinzuzufügen.

Fenster "Vertrauenswürdiges Gerät (Geräte-ID)"

In diesem Fenster können Sie ein Gerät anhand seiner ID zur Liste der vertrauenswürdigen Geräte hinzufügen.

Gerät anhand von ID hinzufügen

Einstellung	Beschreibung
Geräte-ID	Eingabefeld für eine ID oder Maske der Geräte-ID. Sie können die ID manuell eingeben oder die erforderliche Geräte-ID aus der Liste **Auf den Client-Geräten gefundene Geräte** kopieren. Um eine ID anzugeben, können Sie die Platzhalter "*" (beliebige Zeichenfolge) oder "?" (beliebiges einzelnes Zeichen) verwenden. Sie können beispielsweise die Maske "USBSTOR*" angeben, um den Zugriff auf alle USB-Laufwerke zu erlauben.
Kommentar	Eingabefeld für einen Kommentar (optional). Dieses Feld ist nach der Eingabe der Geräte-ID und dem Klick auf **Weiter** verfügbar.

Fenster "Vertrauenswürdiges Gerät (Liste mit erkannten Geräten)"

In diesem Fenster können Sie Geräte zu einer Liste vertrauenswürdiger Geräte hinzufügen, indem Sie es aus der Liste mit dem auf dem verwalteten Client-Gerät gefundenen Geräten auswählen.

Informationen zu vorhandenen Geräten sind nur verfügbar, wenn eine aktive Richtlinie vorhanden ist und eine Synchronisierung mit dem Administrationsagenten stattgefunden hat (wird in dem Intervall ausgeführt, das in den Eigenschaften der Richtlinie des Administrationsagenten festgelegt ist – standardmäßig alle 15 Minuten). Wenn Sie eine neue Richtlinie erstellen und keine anderen Richtlinien aktiv sind, ist die Liste leer.

Gerät aus Liste hinzufügen

Einstellung	Beschreibung
Gerätetyp	In dieser Dropdown-Liste können Sie den Typ der Geräte auswählen, die in der Tabelle **Auf den Client-Geräten gefundene Geräte** angezeigt werden sollen.
Maske der Geräte-ID	Eingabefeld für eine Maske der Geräte-ID.
Kommentar	Eingabefeld für einen Kommentar (optional). Dieses Feld ist verfügbar, sobald Sie mindestens ein Gerät auswählen und auf **Weiter** klicken.

Die Schaltfläche **Filter** öffnet das Fenster, in dem Sie die Filterung der angezeigten Informationen über Geräte anpassen können.

Fenster "Gerätetypen"

In diesem Fenster können Sie die Zugriffsregeln für verschiedene Gerätetypen anpassen.

Zugriffsregeln für Gerätetypen

Einstellung	Beschreibung

Einstellungen für Zugriffe auf Geräte zum Datenspeichern	Folgende Spalten sind in der Tabelle enthalten:
	• **Typ** – Gerätetyp (z. B. Festplatten, Drucker).
	• **Zugriffsmodus** – Zugriffsmodus für Geräte des entsprechenden Typs. Sie können einen der folgenden Zugriffsmodi auswählen:
	  • **Erlauben** – Gewährt Zugriff auf Geräte dieses Typs.
	  • **Blockieren** – Blockiert den Zugriff auf Geräte dieses Typs.
	  • **Je nach Bus** (Standardwert) – Erlaubt oder blockiert den Zugriff auf Geräte abhängig vom Zugriffsmodus für den Bus, der zum Verbinden eines Geräts verwendet wird.
	  • **Auf Regeln basierend** – Erlaubt oder blockiert den Zugriff auf Geräte gemäß Zugriffsregel und Zeitplan. Die Zugriffsregel und ihren Zeitplan können Sie durch Anklicken des geforderten Gerätetyps konfigurieren.

Einstellungen für Zugriffe auf andere Geräte	Folgende Spalten sind in der Tabelle enthalten:
	• **Typ** – Gerätetyp (z. B. Eingabegeräte, Soundkarten).
	• **Zugriffsmodus** – Zugriffsmodus für Geräte des entsprechenden Typs. Sie können einen der folgenden Zugriffsmodi auswählen:
	  • **Erlauben** – Gewährt Zugriff auf Geräte dieses Typs.
	  • **Blockieren** – Blockiert den Zugriff auf Geräte dieses Typs. Für Netzwerkadapter kann der Zugriffsmodus **Blockieren** nicht ausgewählt werden.
	  • **Je nach Bus** (Standardwert) – Erlaubt oder blockiert den Zugriff auf Geräte abhängig vom Zugriffsmodus für den Bus, der zum Verbinden eines Geräts verwendet wird.

Fenster "Einstellungen für Zugriffe auf Geräte"

In diesem Fenster können Sie den Zugriffsmodus und Zugriffsregeln für den ausgewählten Gerätetyp konfigurieren.

Einstellungen für Zugriffe auf Geräte

Einstellung	Beschreibung
Gerätezugriffsmodi	Zugriffsmodus für Geräte des ausgewählten Typs: • **Erlauben** – Gewährt Zugriff auf Geräte des ausgewählten Typs.

	• **Blockieren** – Blockiert den Zugriff auf Geräte des ausgewählten Typs. • **Je nach Bus** (Standardwert) – Erlaubt oder blockiert den Zugriff auf Geräte gemäß einer Zugriffsregel für Bus, der zum Verbinden eines Geräts verwendet wird. • **Auf Regeln basierend** – Erlaubt oder blockiert den Zugriff auf Geräte gemäß einer Zugriffsregel und ihrem Zeitplan.

Gerätezugriffsregeln	Die Tabelle enthält eine Liste der Zugriffsregeln und besteht aus den folgenden Spalten:
	• **Zugriffszeitplan** – Enthält die Namen der vorhandenen Zugriffszeitpläne.
	• **Benutzer und/oder Benutzergruppen** – Enthält die Namen der Benutzer oder Benutzergruppen, auf welche die Zugriffsregel angewendet wird.
	• **Zugriff** – Zugriffsmodus für den Zeitplan:
	  • **Erlauben** (gewährt Zugriff auf Geräte des ausgewählten Typs).
	  • **Blockieren** (sperrt den Zugriff auf Geräte des ausgewählten Typs).
	• **Status** – Ausführungsstatus der Zugriffsregel:
	  • **Aktiviert** – Die Regel ist aktiviert und wird während der Ausführung der Geräte-Kontrolle angewendet.
	  • **Deaktiviert** – Die Regel ist deaktiviert und wird während der Ausführung der Geräte-Kontrolle nicht angewendet.
	Standardmäßig enthält die Tabelle den Zugriffszeitplan **Standard-Zeitplan**, der allen Benutzern vollen Zugriff auf Geräte ermöglicht (in der Liste der Benutzer und Benutzergruppen ist **\Alle** ausgewählt), wenn für diesen Gerätetyp der Zugriff über einen Verbindungsbus aktiviert ist.
	Sie können Zugriffsregeln hinzufügen, bearbeiten und löschen.
	Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.
	Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Fenster "Gerätezugriffsregel"

In diesem Fenster können Sie eine Gerätezugriffsregel anpassen.

Gerätezugriffsregel

Einstellung	Beschreibung
Einstellungen der Gerätezugriffsregel	Zugriffsmodus für Geräte des ausgewählten Typs: • **Erlauben** (Standardwert) – Gewährt Zugriff auf Geräte des ausgewählten Typs. • **Blockieren** – Blockiert den Zugriff auf Geräte des ausgewählten Typs.

Benutzer und/oder Benutzergruppen	Name des Benutzers oder der Benutzergruppe, auf welche die Regel angewendet wird. Der Standardwert ist **\Alle** (alle Benutzer). Sie können Benutzer und Benutzergruppen hinzufügen, anpassen und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.
Status	Ausführungsstatus der Zugriffsregel: • **Aktiviert** – Die Regel ist aktiviert und wird während der Ausführung der Geräte-Kontrolle angewendet. • **Deaktiviert** – Die Regel ist deaktiviert und wird während der Ausführung der Geräte-Kontrolle nicht angewendet.
Zeitplan für Gerätezugriff	Zugriffszeitplan für die angegebenen Benutzer auf die Geräte. Der Standardwert ist **Standardzeitplan**. Sie können einen anderen Zeitplan angeben.

Benutzergruppe oder Fenster auswählen

In diesem Fenster können Sie einen lokalen Benutzer oder Domänenbenutzer bzw. eine Gruppe dieser Benutzer angeben, für die Sie eine Zugriffsregel anpassen möchten.

Konfiguration einer Zugriffsregel

Einstellung	Beschreibung
Manuell	Wenn diese Option ausgewählt ist, müssen Sie im unteren Feld den Namen des lokalen Benutzers oder des Domänenbenutzers oder aber den Namen der Benutzergruppe angeben, auf welche die Gerätezugriffsregel angewendet wird.
Liste mit Gruppen oder Benutzern	Wenn diese Option ausgewählt ist, können Sie entweder im Suchfeld die Suchkriterien für die Namen der Benutzer oder Benutzergruppen eingeben, auf welche die Gerätezugriffsregel angewendet wird, oder den Namen der Benutzergruppe aus der unteren Liste auswählen.

Fenster "Zeitpläne"

In diesem Fenster können Sie den Zeitplan für die ausgewählte Gerätezugriffsregel angeben.

Sie können Zugriffszeitpläne hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Der **Standard-Zeitplan** kann nicht gelöscht werden.

Fenster "Zugriffszeitplan"

In diesem Fenster können Sie die Zugriffszeitpläne für Geräte anpassen. Zeitpläne können nur für Festplatten, Wechseldatenträger, Disketten und CD/DVD-Laufwerke konfiguriert werden.

Wenn das Kontrollkästchen **Zugriff auf Dateien während der Untersuchung blockieren** im Abschnitt **Allgemeine Einstellungen** -> **Einstellungen** deaktiviert ist, kann der Zugriff auf Geräte mithilfe des Zeitplans nicht blockiert werden.

Zeitplan für Gerätezugriff

Einstellung	Beschreibung
Name	Eingabefeld für den Namen des Zugriffszeitplans. Der Zeitplanname muss eindeutig sein.
Zeitintervalle	Eine Tabelle, in welcher Sie Zeitintervalle für den Zeitplan auswählen können (Tage und Stunden). Grün hervorgehobene Intervalle sind im Zeitplan enthalten. Um ein Intervall aus dem Zeitplan auszuschließen, klicken Sie auf die entsprechenden Zellen. Vom Zeitplan ausgeschlossene Intervalle werden grau hervorgehoben. Standardmäßig sind alle Intervalle (24/7) im Zeitplan enthalten.

Fenster "Bus-Verbindungen"

In diesem Fenster können Sie den Zugriffsmodus für Bus-Verbindungen konfigurieren.

Zugriffsmodus für Bus-Verbindungen

Einstellung	Beschreibung
Bus-Verbindung	Die Bus-Verbindung, über die Geräte mit dem Client-Gerät verbunden werden: • **FireWire** • **USB**
Zugriffsmodus	Dieser Schalter legt den Zugriffsmodus auf Geräte fest, die diese Bus-Verbindung nutzen: • **Erlauben** (Standardwert) – Gewährt Zugriff auf Geräte, die über diese Bus-Verbindung verbunden sind. • **Blockieren** – Blockiert den Zugriff auf Geräte, die über diese Bus-Verbindung verbunden sind.

Gerätekontrolle in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie Einstellungen der Gerätekontrolle in den Richtlinieneigenschaften konfigurieren (**Sicherheitskontrolle → Gerätekontrolle**).

Einstellungen der Komponente "Gerätekontrolle"

Einstellung	Beschreibung
Gerätekontrolle aktivieren	Dieser Schalter aktiviert bzw. deaktiviert die Komponente Gerätekontrolle. Das Kontrollkästchen ist standardmäßig aktiviert.
Vertrauenswürdige Geräte	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Vertrauenswürdige Geräte** öffnet. In diesem Fenster können Sie ein Gerät anhand seiner ID zur Liste der vertrauenswürdigen Geräte hinzufügen oder aus der Liste der auf Client-Geräten gefundenen Geräte auswählen.
Ausführungsmodus der Gerätekontrolle	Ausführungsmodus der App beim Zugriffsversuch auf ein Gerät, auf das der Zugriff gemäß den Einstellungen der Gerätekontrolle verboten ist. • **Informieren**. Wenn Sie diese Option auswählen, testet Kaspersky Endpoint Security den ausgewählten Zugriffsmodus und generiert ein Ereignis über den Fund eines Zugriffsversuchs auf das Gerät. • **Blockieren** (Standardwert). Wenn Sie diese Option auswählen, wendet Kaspersky Endpoint Security den für das Gerät oder den Bus angegebenen Zugriffsmodus an.
Einstellungen der Gerätekontrolle	Die Einstellungsgruppe enthält Schaltflächen, die beim Klicken Fenster öffnen, in denen Sie den Zugriffsmodus für Geräte je nach ihrem Typ und den Zugriffsmodus für Bus-Verbindungen konfigurieren können.

Fenster "Vertrauenswürdige Geräte"

Die Tabelle enthält eine Liste der vertrauenswürdigen Geräte. Standardmäßig die Tabelle leer.

Einstellungen eines vertrauenswürdigen Geräts

Einstellung	Beschreibung
Geräte-ID	ID eines vertrauenswürdigen Geräts.
Computername	Name eines vertrauenswürdigen Geräts.
Gerätetyp	Typ eines vertrauenswürdigen Geräts (z. B. Festplatte oder Smartcard-Leser).
Name des Client-Geräts	Name des Client-Geräts, mit dem das vertrauenswürdige Gerät verbunden ist.
Kommentar	Kommentar zu einem vertrauenswürdigen Gerät.

Sie können ein Gerät zu einer Liste vertrauenswürdiger Geräte entweder nach ID oder Maske oder durch Auswahl des gewünschten Geräts aus der Liste der auf dem Benutzergerät gefundenen Geräte hinzufügen.

Sie können vertrauenswürdige Geräte in der Tabelle bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Sie können auch eine Liste von Geräten aus einer Datei importieren, indem Sie auf die Schaltfläche **Erweitert** -> **Importieren** klicken und die Liste der hinzugefügten Geräte über die Schaltflächen **Erweitert** -> **Ausgewählte exportieren** oder **Erweitert** -> **Alle exportieren** in eine Datei exportieren. Beim Importieren wird Ihnen vorgeschlagen, entweder die Liste der vertrauenswürdigen Geräte zu ersetzen oder die Geräte zu einer bestehenden Liste hinzuzufügen.

Fenster "Vertrauenswürdiges Gerät"

In diesem Fenster können Sie ein Gerät anhand seiner ID zur Liste der vertrauenswürdigen Geräte hinzufügen.

Gerät anhand von ID hinzufügen

Einstellung	Beschreibung
Geräte-ID	Eingabefeld für die ID oder ID-Maske des Geräts, das Sie zur Liste der vertrauenswürdigen Geräte hinzufügen möchten. Um eine ID anzugeben, können Sie die Platzhalter "*" (beliebige Zeichenfolge) oder "?" (beliebiges einzelnes Zeichen) verwenden. Sie können beispielsweise die Maske "USBSTOR*" angeben, um den Zugriff auf alle USB-Laufwerke zu erlauben.
Auf Geräten suchen	Durch Klicken auf die Schaltfläche werden die Geräte angezeigt, die anhand der angegebenen ID oder Maske auf den verbundenen Client-Geräten gefunden wurden. Die Schaltfläche ist verfügbar, wenn das Feld **Geräte-ID** einen Wert enthält.
Gefundene Geräte	Folgende Spalten sind in der Tabelle enthalten: • **Gerätetyp** – Der Typ des gefundenen Geräts (z. B. Festplatte oder Smartcard-Reader). • **Geräte-ID** – ID des gefundenen Geräts. • **Gerätename** – Name des gefundenen Geräts. • **Name des Client-Geräts** – Der Name des Client-Geräts, mit dem das gefundene Gerät verbunden ist.
Kommentar	Eingabefeld für den Kommentar zum Gerät, das Sie zur Liste der vertrauenswürdigen Geräte hinzufügen möchten (optional).

Fenster "Geräte an Client-Geräten"

In diesem Fenster können Sie Geräte zu einer Liste vertrauenswürdiger Geräte hinzufügen, indem Sie es aus der Liste mit dem auf dem Client-Gerät gefundenen Geräten auswählen.

Informationen zu vorhandenen Geräten sind nur verfügbar, wenn eine aktive Richtlinie vorhanden ist und eine Synchronisierung mit dem Administrationsagenten stattgefunden hat (wird im Zeitraum ausgeführt, der in der Richtlinie des Administrationsagenten festgelegt ist; standardmäßig 15 Minuten). Wenn Sie eine neue Richtlinie erstellen und keine anderen Richtlinien aktiv sind, ist die Liste leer.

Gerät aus Liste hinzufügen

Einstellung	Beschreibung
Name des Client-Geräts	Eingabefeld für den Namen oder die Namensmasken des verwalteten Geräts, für den Sie nach angeschlossenen Geräten suchen möchten. Die Standardmaske ist * (alle verwaltetet Geräte).
Gerätetyp	In der Dropdown-Liste können Sie den Typ des zu suchenden angeschlossenen Geräts auswählen (z. B. Festplatte oder Smartcard-Leser). Standardmäßig ist die Option **Alle Geräte** ausgewählt.
Geräte-ID	Eingabefeld für die ID oder die Maske der ID des Geräts, das Sie suchen. Die Standardmaske ist * (alle Geräte).
Auf Geräten suchen	Wenn Sie auf diese Schaltfläche klicken, sucht die App nach Geräten mit den angegebenen Parametern. Die Suchergebnisse werden in der Tabelle darunter angezeigt.

Fenster "Gerätetyp"

In diesem Fenster können Sie den Zugriffsmodus für verschiedene Gerätetypen anpassen.

Zugriffsmodus für Gerätetypen

Einstellung	Beschreibung
Gerätetyp	Gerätetyp (z. B. Festplatten, Drucker).
Zugriffsmodus	Zugriffsmodus auf das Gerät Durch Drücken der rechten Maustaste wird das Kontextmenü geöffnet, in dem Sie eine der folgenden Elemente auswählen können: • **Erlauben** – Gewährt Zugriff auf Geräte des ausgewählten Typs. • **Blockieren** – Blockiert den Zugriff auf Geräte des ausgewählten Typs. • **Je nach Bus** (Standardwert) – Erlaubt oder blockiert den Zugriff auf Geräte abhängig vom Zugriffsmodus für die Bus-Verbindung. • **Auf Regeln basierend** – Erlaubt oder blockiert den Zugriff auf Geräte gemäß einer Zugriffsregel und ihrem Zeitplan.

Sie können Zugriffsregeln und Zugriffszeitpläne im Fenster **Konfiguration der Gerätezugriffsregel** konfigurieren, das durch Doppelklicken auf den Namen des Gerätetyps geöffnet wird.

Fenster "Konfiguration der Gerätezugriffsregel"

In diesem Fenster können Sie die Zugriffsregeln und Zeitpläne für den ausgewählten Gerätetyp anpassen.

Das Fenster wird mit einem Doppelklick auf den Namen des Gerätetyps im Fenster **Gerätetyp** geöffnet.

Gerätezugriffsregeln und Zeitpläne

Einstellung	Beschreibung
Benutzer und/oder Benutzergruppen	Eine Liste der Benutzer und Gruppen, für die Sie Zugriffszeitpläne konfigurieren können. Standardmäßig enthält die Tabelle das Element **\Jeder** (alle Benutzer). Sie können Benutzergruppen hinzufügen, anpassen und löschen.
Regeln für die ausgewählte Benutzergruppe nach Zugriffszeitplänen	Die Tabelle enthält Zugriffszeitpläne für Benutzer und Gruppen und besteht aus den folgenden Spalten: • **Zugriffszeitplan** – Enthält die Namen der vorhandenen Zugriffszeitpläne. Das Kontrollkästchen neben dem Zeitplan gibt an, ob dieser Zeitplan von der Komponente verwendet wird. • **Zugriff** – Enthält den Zugriffstyp für den Zeitplan: **Erlauben** (Zugriff auf Geräte des ausgewählten Typs gewähren) oder **Blockieren** (Zugriff auf Geräte des ausgewählten Typs verweigern). Zeitpläne können nur für Festplatten, Wechseldatenträger, Disketten und CD/DVD-Laufwerke konfiguriert werden. Standardmäßig enthält die Tabelle den Zugriffszeitplan **Standard**, der allen Benutzern vollen Zugriff auf Geräte ermöglicht (in der Liste **Benutzer und/oder Benutzergruppen** ist **\Alle** ausgewählt), wenn für diesen Gerätetyp der Zugriff über einen Verbindungsbus aktiviert ist. Für ausgewählte Benutzer können Sie Zugriffszeitpläne hinzufügen, anpassen und löschen. Der Zeitplan **Standard** kann weder geändert noch gelöscht werden. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Fenster "Benutzer oder Gruppe"

In diesem Fenster können Sie den Benutzer oder die Benutzergruppe angeben, für den oder die eine Gerätezugriffsregel gelten soll.

Konfiguration der Gerätezugriffsregel

Einstellung	Beschreibung
Typ	**Benutzer** oder **Gruppe**, für welchen bzw. welche die Regel gilt.
Benutzer- oder Gruppenname	Name des Benutzers oder der Benutzergruppe, für welche die Regel gilt.

Fenster "Zugriffszeitplan"

In diesem Fenster können Sie die Zugriffszeitpläne für Geräte anpassen.

Zeitplan für Gerätezugriff

Einstellung	Beschreibung
Name	Eingabefeld für den Namen des Zugriffszeitplans.

Zeitintervalle	Eine Tabelle, in welcher Sie Zeitintervalle für den Zeitplan auswählen können (Tage und Stunden). Grün hervorgehobene Intervalle sind im Zeitplan enthalten. Um ein Intervall aus dem Zeitplan auszuschließen, klicken Sie auf die entsprechenden Zellen. Vom Zeitplan ausgeschlossene Intervalle werden grau hervorgehoben. Standardmäßig sind alle Intervalle (24/7) im Zeitplan enthalten.

Fenster "Bus-Verbindungen"

In diesem Fenster können Sie den Zugriffsmodus für Bus-Verbindungen konfigurieren.

Zugriffsmodus für Bus-Verbindungen

Einstellung	Beschreibung
Bus-Verbindung	Die Bus-Verbindung, über die Geräte mit dem Client-Gerät verbunden werden: • **FireWire** • **USB**
Zugriffsmodus	Zugriffsmodus für Bus-Verbindungen. Durch Drücken der rechten Maustaste wird das Kontextmenü geöffnet, in dem Sie eine der folgenden Elemente auswählen können: • **Erlauben** (Standardwert) – Gewährt Zugriff auf Geräte, die über diese Bus-Verbindung verbunden sind. • **Blockieren** – Blockiert den Zugriff auf Geräte, die über diese Bus-Verbindung verbunden sind.

Gerätekontrolle über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Gerätekontrolle mithilfe der vordefinierten Aufgabe "Gerätekontrolle" (*Device_Control*) verwalten.

Die Aufgabe "Gerätekontrolle" wird standardmäßig ausgeführt. Sie können diese Aufgabe manuell starten und anhalten.

Sie können die Einstellungen der Gerätekontrolle konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zur Gerätekontrolle ändern.

Sie können die Liste der angeschlossenen Geräte auch mithilfe der Verwaltungsbefehle der Gerätekontrolle anzeigen.

Einstellungen der Aufgabe zur Gerätekontrolle

Die Tabelle beschreibt alle verfügbaren Werte und Standardwerte aller Einstellungen, die Sie für die Aufgabe zur Gerätekontrolle angeben können.

Einstellung	Beschreibung	Wer
OperationMode	Ausführungsmodus der App beim Zugriffsversuch auf ein Gerät, auf das der Zugriff gemäß den Einstellungen der Gerätekontrolle verboten ist.	`Block` (Standard) – Die A Gerät oder den Bus angeg an. `Notify` – Die App testet Zugriffsmodus und generi Fund eines Zugriffsversuc
Der Abschnitt **[DeviceClass]** enthält Zugriffsmodi für Geräte je nach ihrem Typ.		
HardDrive	Legt den Zugriffsmodus für an das Client-Gerät angeschlossene Festplatten fest.	`Allow` – Benutzer haben Festplatten. `DependsOnBus` (Standard die Festplatte hängt vom Bus-Verbindung ab, an die angeschlossen ist. `Block` – Der Zugriff auf a Benutzer blockiert (mit Au Systemfestplatten, die vo nicht blockiert werden). `ByRule` – Der Zugriff auf abhängig von den Zugriffs
RemovableDrive	Legt den Zugriffsmodus für an das Client-Gerät angeschlossene Wechseldatenträger fest.	`Allow` – Benutzer haben Wechseldatenträger. `DependsOnBus` (Standard den Wechseldatenträger Zugriffsmodus für die Bus das Laufwerk angeschlos `Block` – Benutzer haben Wechseldatenträger. `ByRule` – Der Zugriff auf abhängig von den Zugriffs
FloppyDrive	Legt die Zugriffmodi für mit dem Client-Gerät verbundene Disketten fest. Disks, die über eine ISA-Schnittstelle mit dem Client-Gerät verbunden sind, werden von der App nicht blockiert.	`Allow` – Benutzer haben Disketten. `DependsOnBus` (Standard die Diskette hängt vom Zu Bus-Verbindung ab, an die angeschlossen ist. `Block` – Benutzer haben Disketten. `ByRule` – Der Zugriff auf abhängig von den Zugriffs
OpticalDrive	Legt den Zugriffsmodus für CD-/DVD-Laufwerke fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben CD-/DVD-Laufwerke. `DependsOnBus` (Standard den Wechseldatenträger Zugriffsmodus für die Bus das CD-/DVD-Laufwerk a

		`Block` – Benutzer haben CD-/DVD-Laufwerke. `ByRule` – Der Zugriff auf ist abhängig von den Zugr
SerialPortDevice	Legt Zugriffsmodi für Geräte fest, die über eine serielle Schnittstelle an das Client-Gerät angeschlossen sind. Die App blockiert keine Geräte, die über eine serielle Schnittstelle via ISA-Bus an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben die über eine serielle Schr sind. `DependsOnBus` (Standard ein über eine serielle Schr angeschlossenes Gerät is Zugriffsmodus für die Bus `Block` – Benutzer haben Geräte, die über eine serie angeschlossen sind.
ParallelPortDevice	Legt Zugriffsmodi für Geräte fest, die über eine parallele Schnittstelle an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben die über eine parallele Sch angeschlossen sind. `DependsOnBus` (Standard ein über eine parallele Sch angeschlossenes Gerät is Zugriffsmodus für die Bus `Block` – Benutzer haben Geräte, die über eine para Schnittstelle angeschloss
Printer	Legt den Zugriffsmodus für Drucker fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben `DependsOnBus` (Standard den Drucker hängt vom Zu Bus-Verbindung ab, an die angeschlossen ist. `Block` – Benutzer haben Drucker.
Modem	Legt den Zugriffsmodus für Modems fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben `DependsOnBus` (Standard das Modem hängt vom Zu Bus-Verbindung ab, an die angeschlossen ist. `Block` – Benutzer haben Modems.
TapeDrive	Legt den Zugriffsmodus für Bandgeräte fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Bandgeräte. `DependsOnBus` (Standard das Bandgerät hängt vom Bus-Verbindung ab, an die angeschlossen ist. `Block` – Benutzer haben Bandgeräte.
MultifuncDevice	Legt den Zugriffsmodus für Multifunktionsgeräte	`Allow` – Benutzer haben Multifunktionsgeräte.

	fest, die an das Client-Gerät angeschlossen sind.	`DependsOnBus` (Standard das Multifunktionsgerät h Zugriffsmodus für die Bus das Gerät angeschlossen `Block` – Benutzer haben Multifunktionsgeräte.
SmartCardReader	Legt den Zugriffsmodus für Smartcard-Leser fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Smartcard-Leser. `DependsOnBus` (Standard den Smartcard-Leser hän für die Bus-Verbindung ab angeschlossen ist. `Block` – Benutzer haben Smartcard-Leser.
WiFiAdapter	Legt den Zugriffsmodus für WLAN-Adapter fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Adapter. `DependsOnBus` (Standard den WLAN-Adapter ist ab Zugriffsmodus für die Bus `Block` – Benutzer haben WLAN-Adapter.
NetworkAdapter	Legt den Zugriffsmodus für externe Netzwerkadapter fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Netzwerkadapter. `DependsOnBus` (Standard den externen Netzwerkad Zugriffsmodus für die Bus der Adapter angeschlosse Die Gerätekontrolle blo Zugriff auf externe Net Trennung des Client-Ge zu vermeiden.
PortableDevice	Legt den Zugriffsmodus für tragbare Geräte fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben tragbaren Geräte. `DependsOnBus` (Standard das tragbare Gerät hängt die Bus-Verbindung ab, an angeschlossen ist. `Block` – Benutzer haben tragbare Geräte.
BluetoothDevice	Legt den Zugriffsmodus für Bluetooth-Geräte fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Bluetooth-Geräte. `DependsOnBus` (Standard das Bluetooth-Gerät häng für die Bus-Verbindung ab angeschlossen ist. `Block` – Benutzer haben Bluetooth-Geräte.

ImagingDevice	Legt den Zugriffsmodus für Bildverarbeitungsgeräte fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Bildverarbeitungsgeräte. `DependsOnBus` (Standard das Bildverarbeitungsgerä Zugriffsmodus für die Bus das Gerät angeschlossen `Block` – Benutzer haben Bildverarbeitungsgeräte.
SoundAdapter	Legt den Zugriffsmodus für Soundadapter fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Soundadapter. `DependsOnBus` (Standard den Soundadapter hängt die Bus-Verbindung ab, ar angeschlossen ist. `Block` – Benutzer haben Soundadapter.
InputDevice	Legt den Zugriffsmodus für Eingabegeräte (Tastatur, Maus, Touchpad usw.) fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Eingabegeräte. `DependsOnBus` (Standard das Eingabegerät hängt v die Bus-Verbindung ab, ar angeschlossen ist. `Block` – Benutzer haben Eingabegeräte.
Der Abschnitt **[DeviceBus]** enthält Zugriffsmodi für Bus-Verbindungen.		
USB	Zugriffsmodus für Geräte, die über eine USB-Schnittstelle an das Client-Gerät angeschlossen sind.	`Allow` (Standardwert) – auf alle USB-Geräte. `Block` – Benutzer haben Geräte.
FireWire	Zugriffsmodus für Geräte, die über eine FireWire-Schnittstelle an das Client-Gerät angeschlossen sind.	`Allow` (Standardwert) – auf alle Geräte, die über e Schnittstelle angeschloss `Block` – Benutzer haben Geräte, die über eine Fire angeschlossen sind.
Der Abschnitt **[TrustedDevices.item_#]** enthält vertrauenswürdige Geräte.		
DeviceId	Gibt die ID oder ID-Maske eines vertrauenswürdigen Geräts an.	Sie können die Masken * (oder ? (ein beliebiges Zeic Geräte-ID anzugeben. Beispiele: *Um den Zugriff auf alle dem angegebenen zu v die folgenden Paramete Im Abschnitt `[DeviceE USB=Block` Im Abschnitt `[Trusted` den Parameter `Device` gewünschten Geräts

		Um den Zugriff auf säm verweigern, und nur auf zuzulassen, geben Sie d Parameter an: Im Abschnitt `[DeviceE` `USB=Block` Im Abschnitt `[Trusted` den Parameter `Device`
Comment	Kommentar zum angegebenen vertrauenswürdigen Gerät.	—
Der Abschnitt **[Schedules.item_#]** enthält die Zugriffszeitpläne für Geräte. Sie können die Zeitpläne nur für Fest Wechseldatenträger, Disketten und CD/DVD-Laufwerke konfigurieren.		
ScheduleName	Gibt den Namen eines Zeitplans an. Der Zeitplanname muss eindeutig sein.	Standardwert: `Default`. Der Zeitplan `Default` ern jederzeit den vollständige sofern der Zugriff über de den jeweiligen Gerätetyp Der `Standard-` Zeitplan k werden.

DaysHours	Gibt die Zeitintervalle für einen Zeitplan an.	`All` (Standardwert) – De (keine zeitliche Begrenzur
		
		`< week_day >` – Wochent die vollständigen Namen d auch deren Abkürzungen können Sie für Montag die `Monday` angeben). Für die Sie Intervalle oder bestim Woche beginnt am Sonnt
		
		`< hour >` – Stunden [0:24 Sie nur Intervalle angeben
		
		Beispiele:
		So legen Sie den Zeitpla der die Tage von Sonnt bis 11, von 12 bis 15 und v
		`[Schedules.item_00`
		`ScheduleName=sched`
		`DaysHours=Su-Sa:0.`
		So legen Sie den Zeitpla der die folgenden Interv Donnerstag von 12 bis 1 und von 16 bis 24:
		`[Schedules.item_00`
		`ScheduleName=sched`
		`DaysHours=Th:12..1`
		So legen Sie den Zeitpla der 24 Stunden und 7 T abdeckt:
		`[Schedules.item_00`

		`ScheduleName=sched` `DaysHours=All`
Der Abschnitt **[HardDrivePrincipals.item_#]** enthält die Zugriffsregeln für Festplatten. Für Festplatten muss immer mindestens ein Zeitplan aktiviert sein. Einer Festplatte können mehrere Zugriffsregel Es können auch mehrere Zeitpläne für einen Benutzer oder eine Benutzergruppe angegeben werden. Bei Konflikte für Benutzer und Gruppen werden minimal mögliche Zugriffsrechte gewährt.		
Principal	Gibt einen Benutzer oder eine Benutzergruppe an, für welche die Zugriffsregel gelten soll.	`.\Everyone` (Standardwe gilt für alle Benutzer `< Benutzername >` – Nam den die Zugriffsregel gilt. `@< Gruppenname >` – Nam Benutzern, für welche die
[HardDrivePrincipals.item_#.AccessRules.item_#]	Einstellungen der Zugriffsregel.	–
UseRule	Gibt an, ob die Regel aktiviert oder deaktiviert ist.	`Yes` (Standardwert) – Die aktiviert. `No` – Die Zugriffsregel ist
ScheduleName	Gibt den im Abschnitt [Schedules.item_#] festgelegten Zeitplan an.	Standardwert: `Default`.
Access	Gibt den Zugriffstyp an.	`Allow` (Standardwert) – D Festplatten ist erlaubt. `Block` – der Zugriff auf F blockiert.
Der Abschnitt **[RemovableDrivePrincipals.item_#]** enthält die Zugriffsregeln für Wechseldatenträger. Für Wechseldatenträger muss immer mindestens ein Zeitplan aktiviert sein. Einem Wechseldatenträger können m zugewiesen werden. Es können auch mehrere Zeitpläne für einen Benutzer oder eine Benutzergruppe angegeben den Zugriffsplänen für Benutzer und Gruppen werden minimal mögliche Zugriffsrechte gewährt.		
Principal	Gibt einen Benutzer oder eine Benutzergruppe an, für welche die Zugriffsregel gelten soll.	`.\Everyone` (Standardwe gilt für alle Benutzer `< Benutzername >` – Nam den die Zugriffsregel gilt. `@< Gruppenname >` – Nam Benutzern, für welche die
[RemovableDrivePrincipals.item_#.AccessRules.item_#]	Einstellungen der Zugriffsregel.	–
UseRule	Gibt an, ob die Regel aktiviert oder deaktiviert ist.	`Yes` (Standardwert) – Die aktiviert. `No` – Die Zugriffsregel ist
ScheduleName	Gibt den im Abschnitt [Schedules.item_#] festgelegten Zeitplan an.	Standardwert: `Default`.
Access	Gibt den Zugriffstyp an.	`Allow` (Standardwert) – D Festplatten ist erlaubt.

		`Block` – Der Zugriff auf V blockiert.
Der Abschnitt **[FloppyDrivePrincipals.item_#]** enthält die Zugriffsregeln für Diskettenlaufwerke. Für Diskettenlaufwerke muss immer mindestens ein Zeitplan aktiviert sein. Einem Diskettenlaufwerk können mehre zugewiesen werden. Es können auch mehrere Zeitpläne für einen Benutzer oder eine Benutzergruppe angegeben den Zugriffsplänen für Benutzer und Gruppen werden minimal mögliche Zugriffsrechte gewährt.		
Principal	Gibt einen Benutzer oder eine Benutzergruppe an, für welche die Zugriffsregel gelten soll.	`.\Everyone` (Standardwe gilt für alle Benutzer `< Benutzername >` – Nam den die Zugriffsregel gilt. `@< Gruppenname >` – Nam Benutzern, für welche die
[FloppyDrivePrincipals.item_#.AccessRules.item_#]	Einstellungen der Zugriffsregel.	–
UseRule	Gibt an, ob die Regel aktiviert oder deaktiviert ist.	`Yes` (Standardwert) – Die aktiviert. `No` – Die Zugriffsregel ist
ScheduleName	Gibt den im Abschnitt [Schedules.item_#] festgelegten Zeitplan an.	Standardwert: `Default`.
Access	Gibt den Zugriffstyp an.	`Allow` (Standardwert) – D Diskettenlaufwerke ist erla `Block` – Der Zugriff auf D blockiert.
Der Abschnitt **[OpticalDrivePrincipals.item_#]** enthält die Zugriffsregeln für CD-/DVD-Laufwerke. Für CD-/DVD-Laufwerke muss immer mindestens ein Zeitplan aktiviert sein. Einem CD-/DVD-Laufwerk können m zugewiesen werden. Es können auch mehrere Zeitpläne für einen Benutzer oder eine Benutzergruppe angegeben den Zugriffsplänen für Benutzer und Gruppen werden minimal mögliche Zugriffsrechte gewährt.		
Principal	Gibt einen Benutzer oder eine Benutzergruppe an, für welche die Zugriffsregel gelten soll.	`.\Everyone` (Standardwe gilt für alle Benutzer `< Benutzername >` – Nam den die Zugriffsregel gilt. `@< Gruppenname >` – Nam Benutzern, für welche die
[OpticalDrivePrincipals.item_#.AccessRules.item_#]	Einstellungen der Zugriffsregel.	–
UseRule	Gibt an, ob die Regel aktiviert oder deaktiviert ist.	`Yes` (Standardwert) – Die aktiviert. `No` – Die Zugriffsregel ist
ScheduleName	Gibt den im Abschnitt [Schedules.item_#] festgelegten Zeitplan an.	Standardwert: `Default`.
Access	Gibt den Zugriffstyp an.	`Allow` (Standardwert) – D CD-/DVD-Laufwerke ist e

		`Block` – Der Zugriff auf C wird blockiert.

Liste der verbundenen Geräte in der Befehlszeile anzeigen

Nur Benutzer mit den Rollen admin und audit dürfen die Liste der angeschlossenen Geräte anzeigen.

Um eine Liste mit den Aufgaben der App anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control [-D] --get-device-list
```

Kaspersky Endpoint Security zeigt folgende Informationen zu den angeschlossenen Geräten an:

- **Gerätetyp**. Der Typ des angeschlossenen Geräts. Zum Beispiel `OpticalDrive` oder `HardDrive`.
- **ID (Kennung)**. ID des angeschlossenen Geräts.
- **Name**. Name des angeschlossenen Geräts.
- **Pfad**. Pfad des Gerätes im virtuellen Betriebssystem sysfs.
- **Systemlaufwerk**. Diese Einstellung gibt an, ob das angeschlossene Gerät ein Systemlaufwerk ist (ja oder nein).
- **Busse**. Bus-Verbindung. Mögliche Werte: `UnknownBus`, `USB`, `FireWire`.
- **Treiber**. Der Name des zu verwendenden Treibers, wie er vom virtuellen Betriebssystem sysfs gelesen wird.

Web-Kontrolle

Die Web-Kontrolle steuert den Benutzerzugriff auf Webressourcen. Dies hilft bei der Reduzierung des verbrauchten Datenverkehrs und der Einschränkung von unangemessenen Tätigkeiten während der Arbeitszeit. Wenn ein Benutzer versucht, eine Website zu öffnen, deren Zugriff durch die Web-Kontrolle eingeschränkt ist, blockiert Kaspersky Endpoint Security den Zugriff oder zeigt eine Warnung an.

Kaspersky Endpoint Security überwacht nur HTTP- und HTTPS-Datenverkehr.

Mit der Web-Kontrolle können Sie den Zugriff auf Websites anhand folgender Methoden konfigurieren:

- Nach Inhaltskategorien. Die Kategorisierung des Inhalts von Websites erfolgt mittels des Cloud-Dienstes Kaspersky Security Network, durch heuristische Analyse und anhand einer Datenbank bekannter Websites (diese ist Teil der App-Datenbank). Sie können beispielsweise den Benutzerzugriff auf die Inhaltskategorie "Soziale Netzwerke" oder auf andere Kategorien beschränken.

- Nach Datentypkategorien. Sie können den Benutzerzugriff nach Datenarten einschränken und beispielsweise Grafiken ausblenden. Die App bestimmt den Datentyp anhand des Dateiformats, nicht anhand der Erweiterung.

  Die App untersucht keine Dateien in Archiven. Wenn beispielsweise Bilddateien archiviert werden, erkennt die App den Datentyp als "Archive" und nicht als "Bilddateien".

- Nach Webadresse. Sie können eine Webadresse oder eine Maske für Webadressen angeben.

Sie können mehrere Methoden verwenden, um den Zugriff auf Websites gleichzeitig zu steuern. Beispielsweise können Sie den Zugriff auf die Datentypkategorie "Dateien von Office-Anwendungen" für die Inhaltskategorie "Web-Mail" beschränken.

Standardmäßig ist für alle Webressourcen die *Standardregel* **Erlauben** ausgewählt. Gemäß dieser Regel erlaubt die Web-Kontrolle den Benutzern den Zugriff auf Webressourcen, sofern keine anderen *Regeln für den Zugriff auf Webressourcen* angegeben sind.

Sie können die Standardregel für die Web-Kontrolle, nach der die App den Zugriff auf Webressourcen reguliert, die nicht durch andere Regeln abgedeckt sind, ändern, und die Standardregel **Blockieren** *festlegen*. Gemäß dieser Regel verbietet die Web-Kontrolle den Benutzern den Zugriff auf Webressourcen, sofern keine anderen *Regeln für den Zugriff auf Webressourcen* angegeben sind.

Über die Zugriffsregeln für Webressourcen

Eine Zugriffsregel auf Webressourcen besteht aus einer Reihe von Filtern und einer Aktion, die von der App angewendet werden, wenn ein Benutzer die in der Regel beschriebenen Webressourcen zu dem im Zeitplan der Regel angegebenen Zeitpunkt besucht. Mithilfe von Filtern können Sie Webressourcen angeben, auf die der Zugriff durch die Komponente "Web-Kontrolle" kontrolliert wird.

Es stehen folgende Filter zur Verfügung:

- **Filter nach Inhaltskategorien** Die Web-Kontrolle kann Webressourcen in Inhaltskategorien aufteilen. Sie können den Benutzerzugriff auf Webressourcen kontrollieren, die durch diese Kategorien definierte Inhalte enthalten. Wenn ein Benutzer eine Webressource besucht, die zu der ausgewählten Inhaltskategorie gehört, führt die App die in der Regel angegebene Aktion aus.

- **Filter nach Datentypkategorien**. Die Web-Kontrolle kann Webressourcen nach Datentypkategorien aufteilen. Sie können den Benutzerzugriff auf bestimmte Arten von Daten kontrollieren, die als Webressourcen

veröffentlicht werden. Wenn ein Benutzer eine Webressource abruft, die zur ausgewählten Datentypkategorie gehört, führt die App die in der Regel angegebene Aktion aus.

- **Filter nach Adressen der Webressourcen**. Sie können den Benutzerzugriff auf alle Adressen einer Webressource, auf einzelne Adressen einer Webressource und/oder für Adressgruppen einer Webressource kontrollieren.

  Wenn sowohl ein Filter nach Inhaltskategorien und/oder Datentypkategorien als auch ein Filter nach Adressen der Webressourcen angegeben ist und die angegebenen Adressen bzw. Adressgruppen der Webressourcen zu den ausgewählten Inhaltskategorien oder Datentypkategorien gehören, kontrolliert die App den Zugriff nicht auf alle Webressourcen der ausgewählten Inhaltskategorien und/oder Datentypkategorien, sondern nur auf die angegebenen Adressen bzw. Adressgruppen von Webressourcen.

- **Filter nach Benutzername und Benutzergruppe**. Sie können Benutzer und/oder Benutzergruppen angeben, für die der Zugriff auf Webressourcen gemäß der Regel gesteuert wird. Beispielsweise können Sie den Internetzugriff mittels Browser auf alle Benutzer der Organisation mit Ausnahme der IT-Abteilung beschränken.

- **Anwendungszeitplan der Regel**. Sie können für die Regel einen Anwendungszeitplan festlegen. Der Anwendungszeitplan der Regeln bestimmt den Zeitpunkt, an dem die App den Zugriff auf die in der Regel angegebenen Webressourcen kontrolliert. Beispielsweise können Sie den Internetzugriff mittels Browser auf die Geschäftszeiten beschränken.

Für jede Regel können Sie die Aktion angeben, die von der Web-Kontrolle ausgeführt wird, wenn ein Benutzer eine Webressource besucht, die den Einstellungen in der Regel entspricht:

- *Erlauben.* Die Web-Kontrolle erlaubt den Benutzerzugriff auf Webressource.

- *Blockieren.* Die Web-Kontrolle verweigert den Benutzerzugriff auf Webressource und zeigt eine Meldung über die Zugriffsverweigerung an.

- *Informieren.* Die Web-Kontrolle zeigt eine Warnung an, dass es nicht empfohlen wird, die Webressource zu besuchen. Mittels eines Links in der Warnmeldung kann der Benutzer auf die angeforderte Webressource zugreifen.

Jede Regel besitzt eine Priorität. Je höher sich eine Regel in der Liste befindet, desto höher ist ihre Priorität. Wird eine Website mehreren Regeln hinzugefügt, regelt die Web-Kontrolle den Zugriff auf diese Website entsprechend der Regel mit der höchsten Priorität. Beispielsweise könnte die App das Web-Portal eines Unternehmens als soziales Netzwerk definieren. Um den Zugriff auf soziale Netzwerke einzuschränken, ohne dabei den Zugriff auf das Web-Portal des Unternehmens zu verlieren, müssen Sie zwei Regeln erstellen: eine Verbotsregel für die Inhaltskategorie "Soziale Netzwerke" und eine Erlaubnisregel für das Web-Portal des Unternehmens. Die Zugriffsregel für das Web-Portal des Unternehmens sollte dabei eine höhere Priorität bekommen als die Zugriffsregel für soziale Netzwerke.

Wenn gar keine Verbotsregel erstellt wurde, wird der HTTPS-Verkehr nicht entschlüsselt.

Die Web-Kontrolle in der Web Console konfigurieren

In der Web Console können Sie Einstellungen der Web-Kontrolle in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen** → **Sicherheitskontrolle** → **Web-Kontrolle**).

Einstellungen der Komponente "Web-Kontrolle"

Einstellung	Beschreibung
Web-	Dieser Umschalter aktiviert bzw. deaktiviert die Web-Kontrolle.

Kontrolle ist aktiviert / deaktiviert	Der Schalter ist standardmäßig deaktiviert.

Regelliste	Die Tabelle enthält eine Liste mit Zugriffsregeln für Webressourcen. Während der Ausführung wendet die Web-Kontrolle die Regeln entsprechend der Reihenfolge an, die in der Tabelle angegeben ist.
	Folgende Spalten sind in der Tabelle enthalten:
	• **Regelname**. Der Name der Zugriffsregel für die Webressourcen.
	• **Status**. Ausführungsstatus der Zugriffsregel für die Webressourcen:
	  • *Aktiviert* – Die Regel ist aktiviert und wird während der Ausführung der Web-Kontrolle angewendet.
	  • *Deaktiviert* – Die Regel ist deaktiviert und wird während der Ausführung der Web-Kontrolle nicht angewendet.
	Sie können den Umschalter in der Tabelle aktivieren oder deaktivieren oder das Kontrollkästchen **Diese Regel anwenden** im Fenster **Regel der Web-Kontrolle** aktivieren oder deaktivieren.
	• **Aktion**. Die Aktion, die von der App ausführt wird, wenn ein Versuch erkennt wird, auf Webressourcen zuzugreifen, die der Regel entsprechen.
	Sie können Elemente in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.
	Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.
	Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.
	Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.
	Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.
	Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.
	Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.
	Sie können auch eine Liste von Regeln aus einer Datei importieren, indem Sie auf die Schaltfläche **Importieren** klicken und die Liste der hinzugefügten Regeln über die Schaltfläche **Exportieren** in eine Datei exportieren. Beim Importieren wird Ihnen vorgeschlagen, entweder die Liste mit Regeln zu ersetzen oder die Regeln zu einer bestehenden Liste hinzuzufügen.

Standard-Regel	Sie können eine Standardregel, nach der die App den Zugriff auf Webressourcen regelt, die keinen anderen Regeln unterliegen, auswählen: • **Alles erlauben, das nicht in der Regelliste angegeben ist** (Standardwert) – Zugriff auf Webressourcen zulassen.

	• **Alles blockieren, das nicht in der Regelliste angegeben ist** – Zugriff auf Webressourcen blockieren.
Vorlagen	**Warnung**. Das Eingabefeld enthält eine Benachrichtigungsvorlage, die beim Auslösen einer Regel angezeigt wird und vor einem Versuch warnt, auf eine nicht empfohlene Webressource zuzugreifen. **Nachricht bei blockiertem Aufruf**. Das Eingabefeld enthält eine Benachrichtigungsvorlage, die angezeigt wird, wenn eine Regel ausgelöst wird, die den Zugriff auf eine Webressource blockiert. **Nachricht an den Administrator**. Das Eingabefeld enthält eine Vorlage für eine Anfrage, die an den Administrator des lokalen Netzwerks der Organisation gesendet werden kann, wenn nach Meinung des Benutzers der Zugriff auf die Webressource irrtümlich blockiert wurde. Nachdem ein Benutzer die Gewährung des Zugriffs beantragt hat, sendet Kaspersky Endpoint Security das Ereignis *Nachricht an den Administrator über den verweigerten Zugriff auf ein Webseiten* an Kaspersky Security Center. Die Ereignisbeschreibung enthält eine an den Administrator gerichtete Nachricht mit ersetzten Variablen. Wenn Kaspersky Security Center in Ihrer Organisation nicht verwendet wird oder keine Verbindung zum Administrationsserver besteht, sendet die App eine Nachricht an die angegebene E-Mail-Adresse des Administrators.

Fenster "Regel der Web-Kontrolle"

In diesem Fenster können Sie die Einstellungen der Regel für den Zugriff auf die Webressourcen anpassen.

Zugriffsregel für Webressourcen hinzufügen

Einstellung	Beschreibung
Regelname	Eingabefeld für den Namen der Zugriffsregel auf die Webressourcen.
Status	Sie können den Status der Zugriffsregel für die Webressourcen auswählen: • *Aktiviert* – Die Regel ist aktiviert und wird während der Ausführung der Web-Kontrolle angewendet. • *Deaktiviert* – Die Regel ist deaktiviert und wird während der Ausführung der Web-Kontrolle nicht angewendet.
Aktion	Sie können die Aktion auswählen, die von der Web-Kontrolle ausgeführt wird, wenn ein Zugriffsversuch auf die Webressource erkannt wird, die der Regel entspricht: • **Erlauben** (Standardwert) – Gewährt Zugriff auf die Webressource. • **Blockieren** – Blockiert den Zugriff auf die Webressource und zeigt eine Meldung über die Zugriffsverweigerung an. • **Informieren** – Zeigt eine Warnung an, dass es nicht empfohlen wird, die Webressource zu besuchen. Mittels eines Links in der Warnmeldung kann der Benutzer auf die angeforderte Webressource zugreifen.
Nach Inhaltskategorien filtern	Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung eines Filters nach Inhaltskategorie. Bei aktiviertem Kontrollkästchen wird der Link **Inhaltskategorien** verfügbar. Wenn Sie diesen klicken, wird ein Fenster geöffnet, in dem Sie die gewünschten Inhaltskategorien auswählen können. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Nach Datentypkategorien filtern	Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung eines Filters nach Inhaltskategorie. Bei aktiviertem Kontrollkästchen wird der Link **Datentypkategorien** verfügbar. Wenn Sie diesen klicken, wird ein Fenster geöffnet, in dem Sie die gewünschten Datentypkategorie auswählen können. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Adressen	Sie können die Verwendungsart eines Adressfilters für Webressourcen auswählen: • **Auf alle Adressen anwenden** (Standardwert). Wenn diese Option ausgewählt ist, wird der Adressfilter für Webressourcen nicht verwendet. Stattdessen wird die Regel der Web-Kontrolle auf die Adressen aller Webressourcen angewendet. • **Auf angegebene Adressen und/oder Gruppen anwenden**. Wenn Sie diese Option auswählen, werden eine Reihe von Elementen verfügbar: Eine Tabelle mit den Adressen der Webressourcen, für welche die Regel gilt. Die Schaltfläche **Adresse hinzufügen**, die ein Fenster öffnet, in dem Sie die erforderlichen Web-Adressen hinzufügen können. Die Schaltfläche **Gruppe hinzufügen**, die das Fenster Adressgruppen öffnet, in dem Sie Adressgruppen für die Webressourcen hinzufügen können.
Benutzer	Für den Filter nach Benutzern, für welche die Zugriffsregel für eine Webressource gelten soll, können Sie die Verwendungsart auswählen: • **Auf alle Benutzer anwenden** (Standardwert). Wenn diese Option ausgewählt ist, wird der Benutzerfilter nicht verwendet. Stattdessen wird die Regel der Web-Kontrolle auf alle Benutzer angewendet. • **Auf angegebene Benutzer und/oder Gruppen anwenden**. Wenn Sie diese Option auswählen, werden eine Reihe von Elementen verfügbar: Die Tabelle der Benutzer und Benutzergruppen, für welche die Regel gelten soll. Die Schaltfläche **Hinzufügen**, die das Fenster **Benutzer oder Gruppen auswählen** öffnet, in welchem Sie die erforderlichen Benutzer und/oder Benutzergruppen hinzufügen können.
Anwendungszeitplan der Regel	Anwendungszeitplan für die Regel der Web-Kontrolle. Der standardmäßige Zeitplan ist **Immer**. Der Link **Immer** öffnet das Fenster **Zeitpläne**, in dem Sie einen anderen Zeitplan für die Regel konfigurieren können.

Fenster "Adressgruppen"

Die Tabelle enthält Gruppen mit Adressen von Webressourcen, auf die der Benutzerzugriff durch die Web-Kontrolle gesteuert wird. Standardmäßig die Tabelle leer.

Konfiguration der Zugriffsregel für die Webressourcen.

Einstellung	Beschreibung
Name der Gruppe	Name der Adressgruppe von Webressourcen, für welche die Regel gilt.
Anzahl an Adressen in der Gruppe	Anzahl an Adressen in der Adressgruppe

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie der Gruppenliste in diesem Fenster eine neue Adressgruppe hinzufügen möchten, öffnen Sie das Fenster Gruppe, indem Sie auf die Schaltfläche **Hinzufügen** klicken, die sich oberhalb der Tabelle befindet.

Wenn Sie im Fenster **Regel der Web-Kontrolle** eine Adressgruppe zur Gruppenliste hinzufügen möchten, aktivieren Sie in der Tabelle das Kontrollkästchen neben dem Gruppennamen und klicken Sie unterhalb der Tabelle auf die Schaltfläche **Gruppen der Regel hinzufügen**.

Fenster "Gruppe"

In diesem Fenster können Sie eine Adressgruppe für Webressourcen hinzufügen.

Konfiguration der Zugriffsregel für die Webressourcen.

Einstellung	Beschreibung
Name der Gruppe	Name der neuen Adressgruppe für Webressourcen.
Adressen	Tabelle der Adressen, die in der Adressgruppe für Webressourcen enthalten sind.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Benutzer oder Gruppe auswählen

In diesem Fenster können Sie einen lokalen Benutzer oder Domänenbenutzer bzw. eine Benutzergruppe angeben, für die Sie eine Zugriffsregel für die Webressource anpassen möchten.

Konfiguration der Zugriffsregel für die Webressourcen.

Einstellung	Beschreibung
Manuell	Wenn diese Option ausgewählt ist, müssen Sie im unteren Feld den Namen des lokalen Benutzers oder des Domänenbenutzers oder aber den Namen der Benutzergruppe angeben, auf welche die Zugriffsregel für Webressourcen angewendet wird.
Liste mit Gruppen oder Benutzern	Wenn diese Option ausgewählt ist, können Sie entweder im Suchfeld die Suchkriterien für die Namen der Benutzer oder Benutzergruppen eingeben, auf welche die Zugriffsregel für Webressourcen angewendet wird, oder den Namen der Benutzergruppe aus der unteren Liste auswählen.

Fenster "Zeitpläne"

In diesem Fenster können Sie den Zeitplan für die ausgewählte Gerätezugriffsregel angeben.

Sie können Zugriffszeitpläne hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Der Standardplan **Immer** kann nichtgelöscht oder geändert werden.

Fenster "Zugriffszeitplan"

In diesem Fenster können Sie die den Zugriffszeitplan für die Webressource anpassen.

Zugriffszeitplan für die Webressourcen.

Einstellung	Beschreibung
Name	Eingabefeld für den Namen des Zugriffszeitplans. Der Zeitplanname muss eindeutig sein.
Zeitintervalle	Eine Tabelle, in welcher Sie Zeitintervalle für den Zeitplan auswählen können (Tage und Stunden). Grün hervorgehobene Intervalle sind im Zeitplan enthalten. Um ein Intervall aus dem Zeitplan auszuschließen, klicken Sie auf die entsprechenden Zellen. Vom Zeitplan ausgeschlossene Intervalle werden grau hervorgehoben. Standardmäßig sind alle Intervalle (24/7) im Zeitplan enthalten.

Die Web-Kontrolle in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie Einstellungen der Web-Kontrolle in den Richtlinieneigenschaften konfigurieren (**Sicherheitskontrolle** → **Web-Kontrolle**).

Einstellungen der Komponente "Web-Kontrolle"

Einstellung	Beschreibung
Web-Kontrolle aktivieren	Das Kontrollkästchen aktiviert die Web-Kontrolle. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Einstellungen der Web-Kontrolle	Die Tabelle enthält eine Liste mit Zugriffsregeln für Webressourcen. Während der Ausführung wendet die Web-Kontrolle die Regeln entsprechend der Reihenfolge an, die in der Tabelle angegeben ist.
	Folgende Spalten sind in der Tabelle enthalten:
	• **Status**. Ausführungsstatus der Zugriffsregel für die Webressourcen:
	  • *Aktiviert* – Die Regel ist aktiviert und wird während der Ausführung der Web-Kontrolle angewendet.
	  • *Deaktiviert* – Die Regel ist deaktiviert und wird während der Ausführung der Web-Kontrolle nicht angewendet.

	Sie können das Kontrollkästchen in der Tabelle aktivieren oder deaktivieren oder das Kontrollkästchen **Diese Regel anwenden** im Fenster Regel der Web-Kontrolle aktivieren oder deaktivieren. • **Aktion**. Die Aktion, die von der App ausführt wird, wenn ein Versuch erkennt wird, auf Webressourcen zuzugreifen, die der Regel entsprechen. • **Name**. Der Name der Zugriffsregel für die Webressourcen. Sie können Elemente in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben. Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Sie können auch eine Liste mit Regeln aus einer Datei importieren, indem Sie auf die Schaltfläche **Erweitert -> Importieren** klicken und die Liste der hinzugefügten Regeln über die Schaltflächen **Erweitert -> Ausgewählte exportieren** oder **Erweitert -> Alle exportieren** in eine Datei exportieren. Beim Importieren wird Ihnen vorgeschlagen, entweder die Liste mit Regeln zu ersetzen oder die Regeln zu einer bestehenden Liste hinzuzufügen.
Standard-Regel	In der Dropdown-Liste können Sie eine Standardregel, nach der die App den Zugriff auf Webressourcen regelt, die keinen anderen Regeln unterliegen, auswählen: • **Erlauben** (Standardwert) – Gewährt Zugriff auf die Webressourcen. • **Blockieren** – Blockiert den Zugriff auf die Webressourcen.
Benachrichtigungsvorlagen	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster Benachrichtigungsvorlagen öffnet.

Fenster "Regel der Web-Kontrolle"

In diesem Fenster können Sie die Einstellungen der Regel für den Zugriff auf die Webressourcenanpassen.

Einstellung	Beschreibung
Regelname	Eingabefeld für den Namen der Zugriffsregel auf die Webressourcen.
Regel anwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Verwendung dieser Regel während der Ausführung der App. Bei aktiviertem Kontrollkästchen ist die Regel aktiviert und die Web-Kontrolle wendet diese Regel während der Ausführung an. Bei deaktiviertem Kontrollkästchen ist die Regel deaktiviert und die Web-Kontrolle wendet diese Regel während der Ausführung nicht an. Sie können die Verwendung dieser Regel durch die Web-Kontrolle aktivieren, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Inhalt filtern	In der Dropdown-Liste können Sie einen Filter für den Inhalt der Webressource auswählen: • **Nicht filtern**(Standardwert). Wenn diese Option ausgewählt ist, wird der Inhaltsfilter für die Webressource nicht verwendet. • **Nach Inhaltskategorien**. Wenn diese Option ausgewählt ist, wird die Schaltfläche **Auswählen** verfügbar. Bei Anklicken der Schaltfläche wird das Fenster **Inhaltskategorien auswählen** geöffnet. • **Nach Datentypkategorien**. Wenn diese Option ausgewählt ist, wird die Schaltfläche **Auswählen** verfügbar. Bei Anklicken der Schaltfläche wird das Fenster **Datentypkategorien auswählen** geöffnet. • **Nach Inhalts- und Datentypkategorien**. Wenn diese Option ausgewählt ist, werden die Schaltflächen **Auswählen** verfügbar. Bei Anklicken der Schaltflächen wird ein Fenster geöffnet, in dem die gewünschten Kategorien ausgewählt werden können.
Adressen filtern	In der Dropdown-Liste können Sie einen Filter für die Adressen der Webressource auswählen: • **Beliebige Adresse** (Standardwert). Wenn diese Option ausgewählt ist, wird der Adressfilter für Webressourcen nicht verwendet. Stattdessen wird die Regel der Web-Kontrolle auf die Adressen aller Webressourcen angewendet. • **Angegebene Adressen**. Wenn dieser Listeneintrag ausgewählt ist, wird die Schaltfläche **Adressen auswählen** verfügbar. Bei Anklicken der Schaltfläche wird das Fenster **Adressen auswählen** geöffnet, in dem die gewünschten Adressen ausgewählt werden können.
Auf diese Benutzer anwenden	In der Dropdown-Liste können die Benutzer ausgewählt werden, für welche die Zugriffsregel der Webressourcen gelten soll: • **Auf alle Benutzer**(Standardwert). Wenn diese Option ausgewählt ist, wird der Benutzerfilter nicht verwendet. Stattdessen wird die Regel der Web-Kontrolle auf alle Benutzer angewendet. • **Auf ausgewählte Benutzer**. Wenn diese Option ausgewählt ist, wird die Schaltfläche **Benutzer auswählen** verfügbar. Bei Anklicken der Schaltfläche wird das Fenster **Benutzerauswahl** geöffnet.
Anwendungszeitplan der Regel	In der Dropdown-Liste können Sie den Anwendungszeitplan der Zugriffsregel für die Webressource konfigurieren:

	• **Immer** (Standardwert). Wenn diese Option ausgewählt ist, wird eine benutzerdefinierte Zugriffsregel für die Webressource ohne zeitliche Einschränkung angewendet, d. h. sie ist immer aktiv. • **<Namen des Zeitplans>**. Wenn diese Option ausgewählt ist, werden die Schaltflächen **Löschen** und **Ändern** verfügbar. Durch Anklicken dieser können Sie diesen Zeitplan löschen oder konfigurieren. • **Neuen Zeitplan hinzufügen**. Wenn diese Option ausgewählt ist, wird das Fenster Zugriffszeitplan geöffnet, in dem Sie den neuen Anwendungszeitplan für den Zugriff auf die Webressource einstellen können.
Aktion der Regel	In der Dropdown-Liste können Sie die Aktion auswählen, die von der Web-Kontrolle ausgeführt wird, wenn ein Zugriffsversuch auf die Webressource erkannt wird, die der Regel entspricht: • **Erlauben** (Standardwert) – Gewährt Zugriff auf die Webressource. • **Blockieren** – Blockiert den Zugriff auf die Webressource und zeigt eine Meldung über die Zugriffsverweigerung an. • **Informieren** – Zeigt eine Warnung an, dass es nicht empfohlen wird, die Webressource zu besuchen. Mittels eines Links in der Warnmeldung kann der Benutzer auf die angeforderte Webressource zugreifen.

Inhaltskategorien auswählen

In diesem Fenster können Sie Inhaltskategorien für Webressourcen auswählen, auf die Sie den Zugriff kontrollieren möchten.

Aktivieren Sie dazu die Kontrollkästchen neben den gewünschten Kategorien.

Standardmäßig sind alle Kontrollkästchen deaktiviert.

Wenn Sie für eine Haupt-Inhaltskategorie die Kontrollkästchen aller ihrer unterordneten Inhaltskategorien aktivieren, wird das Kontrollkästchen der Haupt-Inhaltskategorie nicht automatisch aktiviert.

Datentypkategorien auswählen

In diesem Fenster können Sie Datentypkategorien für Webressourcen auswählen, auf die Sie den Zugriff kontrollieren möchten.

Aktivieren Sie dazu die Kontrollkästchen neben den gewünschten Kategorien.

Alle Kontrollkästchen sind standardmäßig deaktiviert.

Adressen auswählen

In diesem Fenster können Sie Adressen von Webressourcen angeben, auf die Sie den Zugriff kontrollieren möchten. Wenn Sie mehrere Adressen angeben, geben Sie jede Adresse in einer neuen Zeile ein, um sie einfacher kopieren zu können. Für die Angabe der Adressen können Sie Masken verwenden.

Wenn Sie eine Adressgruppe angeben möchten, öffnen Sie das Fenster **Adressgruppen auswählen**, indem Sie auf die Schaltfläche **Adressgruppe hinzufügen** klicken.

Adressgruppen auswählen

Die Tabelle enthält Gruppen mit Adressen von Webressourcen, auf die der Benutzerzugriff durch die Web-Kontrolle gesteuert wird.

Wenn Sie im Fenster **Adressen auswählen** eine Adressgruppe zur Gruppenliste hinzufügen möchten, aktivieren Sie in der Tabelle das Kontrollkästchen neben dem Gruppennamen und klicken Sie unterhalb der Tabelle auf die Schaltfläche **Hinzufügen**.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Wenn Sie der Gruppenliste in diesem Fenster eine neue Adressgruppe hinzufügen möchten, öffnen Sie das Fenster **Adressgruppen hinzufügen**, indem Sie auf die Schaltfläche **Hinzufügen** klicken, die sich oberhalb der Tabelle befindet.

Standardmäßig die Tabelle leer.

Adressgruppen hinzufügen

In diesem Fenster können Sie Adressgruppen von Webressourcen angeben, auf die Sie den Zugriff kontrollieren möchten. Wenn Sie in einer Adressgruppe mehrere Adressen angeben möchten, geben Sie jede Adresse in einer neuen Zeile ein, um sie einfacher kopieren zu können. Für die Angabe der Adressen können Sie Masken verwenden.

Benutzer auswählen

Die Tabelle enthält Namen und Gruppen von Benutzern, für die der Zugriff auf Webressourcen gemäß der Regel gesteuert wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Wenn Sie der Benutzerliste in diesem Fenster einen neuen Benutzer und/oder eine neue Benutzergruppe hinzufügen möchten, öffnen Sie durch Klicken auf die Schaltfläche **Hinzufügen** oberhalb der Tabelle das Fenster **Benutzer oder Gruppe**.

Standardmäßig die Tabelle leer.

Fenster "Benutzer oder Gruppe"

In diesem Fenster können Sie den Benutzer oder die Benutzergruppe angeben, für den oder die eine Zugriffsregel für Webressourcen gelten soll.

Konfiguration der Zugriffsregel für die Webressourcen.

Einstellung	Beschreibung
Typ	**Benutzer** oder **Gruppe**, für welchen bzw. welche die Regel gilt.
Benutzer- oder Gruppenname	Name des Benutzers oder der Benutzergruppe, für welche die Regel gilt.

Fenster "Zugriffszeitplan"

In diesem Fenster können Sie die den Zugriffszeitplan für die Webressource anpassen.

Zugriffszeitplan für die Webressourcen.

Einstellung	Beschreibung
Name	Eingabefeld für den Namen des Zugriffszeitplans.
Zeitintervalle	Eine Tabelle, in welcher Sie Zeitintervalle für den Zeitplan auswählen können (Tage und Stunden). Grün hervorgehobene Intervalle sind im Zeitplan enthalten. Um ein Intervall aus dem Zeitplan auszuschließen, klicken Sie auf die entsprechenden Zellen. Vom Zeitplan ausgeschlossene Intervalle werden grau hervorgehoben. Standardmäßig sind alle Intervalle (24/7) im Zeitplan enthalten.

Benachrichtigungsvorlagen der Web-Kontrolle konfigurieren

Abhängig von der Aktion, die in den Eigenschaften der Regel für die Web-Kontrolle angegeben ist, zeigt die App beim Zugriffsversuch eines Benutzers auf Webressourcen eine Nachricht an (die Antwort des HTTP-Servers wird durch eine HTML-Seite mit einer Nachricht ersetzt), der folgenden Typen entsprechen kann:

- Warnmeldung. Diese Meldung warnt den Benutzer, dass der Besuch der Webressource nicht empfohlen wird und/oder nicht den Sicherheitsrichtlinien des Unternehmens entspricht. Die App zeigt eine Warnmeldung an, wenn in den Einstellungen der Regel für diese Webressource die Aktion **Informieren** ausgewählt ist.

  Sollte die Warnung nach Ansicht des Benutzers irrtümlich angezeigt werden, kann der Benutzer über einen in der Warnmeldung enthaltenen Link eine bereits vorformulierte Anfrage an den Administrator des lokalen Netzwerks der Organisation senden.

- Nachricht über die Blockierung eine Webressource. Die App zeigt eine Meldung über das Blockieren einer Webressource an (siehe Abbildung unten), wenn in den Einstellungen der Regel für diese Webressource die Aktion **Blockieren** ausgewählt ist.

  Sollte die Blockierung des Zugriffs auf die Webressource nach Ansicht des Benutzers irrtümlich geschehen sein, kann der Benutzer über einen in der Nachricht enthaltenen Link eine bereits vorformulierte Anfrage an den Administrator des lokalen Netzwerks der Organisation senden.

Für die Warnmeldung, die Nachricht über das Blockieren des Zugriffs auf eine Webressource und die Anfrage an den Administrator des lokalen Netzwerks der Organisation sind bereits erstellte Vorlagen verfügbar. Sie können deren Inhalt anpassen.

So passen Sie eine Benachrichtigungsvorlage in der Web Console an:

1. Wählen Sie im Hauptfenster von Web Console **Assets (Geräte)** → **Richtlinien und Richtlinienprofile**.

   Die Liste mit Richtlinien wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die die Geräte enthält, auf die die Richtlinie angewendet wird. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

   In der Liste werden die Richtlinien angezeigt, die für die ausgewählte Administrationsgruppe konfiguriert sind.

3. Klicken Sie in der Liste auf den Namen der erforderlichen Richtlinie.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.

4. Wählen Sie im Eigenschaftenfenster der Richtlinie die Option **App-Einstellungen** → **Sicherheitskontrolle** → **Web-Kontrolle** aus.

5. Konfigurieren Sie im Block **Vorlagen** die Benachrichtigungsvorlagen der Web-Kontrolle auf den folgenden Registerkarten:

   - **Warnung**. Das Eingabefeld enthält eine Benachrichtigungsvorlage, die beim Auslösen einer Regel angezeigt wird und vor einem Versuch warnt, auf eine nicht empfohlene Webressource zuzugreifen.

   - **Nachricht bei blockiertem Aufruf**. Das Eingabefeld enthält eine Benachrichtigungsvorlage, die angezeigt wird, wenn eine Regel ausgelöst wird, die den Zugriff auf eine Webressource blockiert.

   - **Nachricht an den Administrator**. Das Eingabefeld enthält eine Vorlage für eine Anfrage, die an den Administrator des lokalen Netzwerks der Organisation gesendet werden kann, wenn nach Meinung des Benutzers der Zugriff auf die Webressource irrtümlich blockiert wurde. Nachdem ein Benutzer die Gewährung des Zugriffs beantragt hat, sendet Kaspersky Endpoint Security das Ereignis *Nachricht an den Administrator über den verweigerten Zugriff auf ein Webseiten* an Kaspersky Security Center. Die Ereignisbeschreibung enthält eine an den Administrator gerichtete Nachricht mit ersetzten Variablen. Wenn Kaspersky Security Center in Ihrer Organisation nicht verwendet wird oder keine Verbindung zum Administrationsserver besteht, sendet die App eine Nachricht an die angegebene E-Mail-Adresse des Administrators.

6. Klicken Sie auf **OK**.

7. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

So passen Sie eine Benachrichtigungsvorlage in der Verwaltungskonsole an:

1. Öffnen Sie in der Struktur der Verwaltungskonsole im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu der die erforderlichen Geräte gehören.

2. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.

3. Wählen Sie in der Liste der Richtlinien die erforderliche Richtlinie aus und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>** mit einem Doppelklick.

   Sie können das Fenster mit den Richtlinieneigenschaften auch über den Eintrag **Eigenschaften** im Kontextmenü der Richtlinie oder durch Klicken auf den Link **Richtlinieneinstellungen konfigurieren** rechts neben der Liste der Richtlinien im Block mit den Richtlinieneinstellungen öffnen.

4. Wählen Sie im Fenster der Richtlinie die Option **Sicherheitskontrolle → Web-Kontrolle** aus.

5. Klicken Sie im Abschnitt **Benachrichtigungsvorlagen** auf die Schaltfläche **Anpassen**.

6. Passen Sie im neuen Fenster **Benachrichtigungsvorlagen** die Benachrichtigungsvorlagen der Web-Kontrolle auf den folgenden Registerkarten an:

   - **Warnung**. Das Eingabefeld enthält eine Benachrichtigungsvorlage, die beim Auslösen einer Regel angezeigt wird und vor einem Versuch warnt, auf eine nicht empfohlene Webressource zuzugreifen.

   - **Nachricht bei blockiertem Aufruf**. Das Eingabefeld enthält eine Benachrichtigungsvorlage, die angezeigt wird, wenn eine Regel ausgelöst wird, die den Zugriff auf eine Webressource blockiert.

   - **Anfrage an den Administrator**. Das Eingabefeld enthält eine Vorlage für eine Anfrage, die an den Administrator des lokalen Netzwerks der Organisation gesendet werden kann, wenn nach Meinung des Benutzers der Zugriff auf die Webressource irrtümlich blockiert wurde. Nachdem ein Benutzer die Gewährung des Zugriffs beantragt hat, sendet Kaspersky Endpoint Security das Ereignis *Nachricht an den Administrator über den verweigerten Zugriff auf ein Webseiten* an Kaspersky Security Center. Die Ereignisbeschreibung enthält eine an den Administrator gerichtete Nachricht mit ersetzten Variablen. Sie können diese Ereignisse in der Konsole von Kaspersky Security Center mithilfe der voreingestellten Auswahl **Benutzeranfragen** anzeigen. Wenn Kaspersky Security Center in Ihrer Organisation nicht verwendet wird oder keine Verbindung zum Administrationsserver besteht, sendet die App eine Nachricht an die angegebene E-Mail-Adresse des Administrators.

7. Klicken Sie auf **OK**.

8. Klicken Sie auf **Übernehmen**.

Die Web-Kontrolle über die Befehlszeile konfigurieren

Sie können die Web-Kontrolle über die Befehlszeile mithilfe der voreingestellten Aufgabe zur Web-Kontrolle (*Web_Control*) verwalten.

Die Aufgabe zur Web-Kontrolle ist standardmäßig gestoppt. Sie können diese Aufgabe manuell starten und anhalten.

Sie können Einstellungen der Web-Kontrolle konfigurieren, indem Sie die Einstellungen der voreingestellten Aufgabe zur Web-Kontrolle ändern.

Sie können Einstellungen der Web-Kontrolle auch mithilfe der Verwaltungsbefehle der Web-Kontrolle anzeigen und konfigurieren.

Einstellungen der Aufgabe "Web-Kontrolle"

Die untere Tabelle beschreibt alle verfügbaren Werte und Standardwerte aller Einstellungen, die Sie für die Aufgabe zur Web-Kontrolle angeben können.

Einstellungen der Aufgabe "Web-Kontrolle"

Einstellung	Beschreibung	Werte
`WebControlDefaultAction`	Die Aktion der	`Allow` (Standardwert) – Gewäh

	Standardregel, welche die Webkontrolle ausführt, wenn sie einen Versuch erkennt, auf Webressourcen zuzugreifen, die nicht durch andere Regeln abgedeckt sind.	Zugriff auf die Webressourcen. `Block` – Verbietet den Zugriff a die Webressourcen.
`ComplaintRecipient`	Die E-Mail-Adresse des Administrators, um ihm eine Anfrage über eine irrtümliche Blockierung einer Webressource zu senden.	
Der Abschnitt **[Rules.item_#]** enthält folgende Einstellungen:		
`Name`	Der Name der Zugriffsregel für die Webressourcen.	
`WebControlAction`	Die Aktion der Regel, die von der Web-Kontrolle ausgeführt wird, wenn ein Zugriffsversuch auf die Webressource erkannt wird, die der Regel entspricht.	`Allow` (Standardwert) – Gewäh Zugriff auf die Webressource. `Block` – Verbietet den Zugriff a die Webressource. `Notify` – Zeigt eine Warnung a dass es nicht empfohlen wird, di Webressource zu besuchen. Mit eines Links in der Warnmeldung kann der Benutzer auf die angeforderte Webressource zugreifen.
`Enabled`	Ausführungsstatus der Zugriffsregel für die Webressourcen:	`Yes` – Die Regel ist aktiviert und wird während der Ausführung de Web-Kontrolle angewendet. `No` (Standardwert) – Die Regel i deaktiviert und wird während de Ausführung der Web-Kontrolle nicht angewendet.
`ScheduleId`	ID des Zeitplans, die im Abschnitt `[Schedules.item_#]` verwendet wird.	
`UseUrls`	Anwenden eines Adressfilters für Webressourcen in der Regel.	`Yes` – Adressfilters für Webressourcen in der Regel anwenden. `No` (Standardwert) – Adressfilte für Webressourcen in der Regel nicht anwenden. Stattdessen w die Regel auf alle Adressen von Webressourcen angewendet.
`Urls.item_#`	Adresse der Webressource, deren Zugriff durch die Regel verwaltet wird.	Zum Angeben der Adressen der Webressourcen können Sie Mas verwenden.

`UseCategories`	Anwenden von Filtern nach Inhaltskategorien und nach Datentypkategorien in der Regel.	`Keine` (Standardwert) – Keine Inhaltsfilter für die Webressourc anwenden. `ContentOnly` – Filter nach Inhaltskategorien in der Regel anwenden. `FormatOnly` – Filter nach Datentypkategorien in der Rege anwenden. `ContentAndFormat` – Filter na Inhaltskategorien und nach Datentypkategorien in der Rege anwenden.
`[Rules.item_#.ContentCategories.item_#]`	Abschnitt zur Angabe der Inhaltskategorie.	–

`ContentCategory`	Inhaltskategorie.	`AdultContent, AlcoholTobaccoNarcotics`
		`Violence, Profanity, Weap`
		`ChatForum, WebMail, OnlineShops`
		`SocialNets, Recruitment`
		`HttpQueryRedirection, CreditCards`
		`PoliceDecision, SoftwareAudioVideo`
		`TechnologyElectronics`
		`GamblingLotteriesSweepsta`
		`InternetCommunicationMedi`
		`CryptocurAndMining, LegislationBE`
		`ECommerce, ComputerGames, Religions`
		`News, Torrents, FileShari`
		`AudioAndVideo, BankSites, Blogs`
		`DatingSites, LegislationR`
		`LegislationGlobal, SexuallyExplicit`
		`Sexuality, GenerativeAITools`

`[Rules.item_#.FormatCategories.item_#]`	Abschnitt zur Angabe der Datentypkategorien.	–
`FormatCategories.item_#.FormatCategory`	Datentypkategorie	`Video` – Video `Audio` – Audiodaten `OfficeDocument` – Dateien vo Office-Anwendungen

		`Executable` – Ausführbare Dateien `Archives` – Archive `Images` – Bilder `Scripts` – Skripte
`UsePrincipals`	Anwenden eines Filters nach Benutzern, für welche die Zugriffsregel für eine Webressource gelten soll.	`Yes` – Filter nach Benutzern in c Regel anwenden. `No` (Standardwert) – Filter nach Benutzern nicht anwenden. Stattdessen wird die Regel auf a Benutzer angewendet.
`[Rules.item_#.Principals.item_#]`	Abschnitt zum Angeben der Benutzer, für welche die Zugriffsregel für die Webressourcen gelten soll.	
`isGroup`	Der Parameter gibt an, ob der im Feld `Name` angegebene Name der Name eines Benutzers oder einer Benutzergruppe ist	`Yes` – Der angegebene Name is Gruppenname. `No` – Der angegebene Name ist Benutzername.
`Name`	Ein Benutzer oder eine Gruppe von Benutzern, für welche die Zugriffsregel für Webressourcen gilt.	`< Benutzername >` – Name des Benutzers, für den die Regel gilt `@< Gruppenname >` – Name der Benutzergruppe, für welche die Regel gilt.
`Sid`	ID des Benutzers oder der Benutzergruppe.	
Der Abschnitt **[UrlCategories.item_#]** enthält folgende Einstellungen:		
`Name`	Der Name der Adressgruppe für Webressourcen, auf welche die Regel den Zugriff verwaltet.	
`Urls.item_#`	Die Adresse einer Webressource, die in der Gruppe enthalten ist.	Zum Angeben der Adressen der Webressourcen können Sie Mas verwenden.
Der Abschnitt **[Schedules.item_#]** enthält den Anwendungszeitplan der Regel.		
`Id`	ID des Zeitplans, die im Abschnitt `[Rules.item_#]` verwendet wird.	`1 - 999999` `0` -ID des Zeitplans `Default` (Standardwert), der sicher stellt dass die Regel ohne zeitliche Einschränkungen ausgeführt wir d. h. sie ist immer aktiv.
`Name`	Gibt den Namen eines	

	Zeitplans an.	
`DaysHours`	Gibt die Zeitintervalle für einen Zeitplan an.	`< week_day >` – Wochentage. S können sowohl die vollständigen Namen der Wochentage als auc deren Abkürzungen verwenden (bspw. können Sie für Montag di Werte `Mo`, `Mon` oder `Monday` angeben). Für die Wochentage können Sie Intervalle oder bestimmte Tage angeben. Die Woche beginnt am Sonntag. `< hour >` – Stunden [0:24]. Für Stunden können Sie nur Interval angeben.

Einstellungen der Web-Kontrolle anzeigen und ändern

Um die Einstellungen der Web-Kontrolle anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 26 [--file <Pfad zur Konfigurationsdatei>] [--json]
```

Wobei gilt:

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, in der die Einstellungen ausgegeben werden.

`--json` – Gibt Daten im JSON-Format aus.

Um die Einstellungen der Web-Kontrolle zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 26 [--file <Pfad zur Konfigurationsdatei>] [--json]
```

Wobei gilt:

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die Einstellungen importiert werden.

`--json` – Importiert die Daten aus einer Datei im JSON-Format importiert.

Führen Sie den folgenden Befehl aus, um die konfigurierten Einstellungen zu löschen und die Werte für die Einstellungen der Web-Kontrolle auf die Standardregel zurückzusetzen:

```
kesl-control --set-settings 26 --set-to-default
```

Regeln zum Definieren von Adressmasken für Webressourcen

Die Verwendung einer *Adressmasken für eine Webressource* (im Weiteren auch "Adressmaske") kann in praktisch sein, wenn Sie beim Erstellen einer Zugriffsregel für Webressourcen viele ähnlich lautende Adressen von Webressourcen eingeben müssen. So kann eine entsprechend formulierte Adressmaske viele Adressen von Webressourcen ersetzen.

Beim Erstellen einer Adressmaske sollten folgende Regeln beachtet werden:

1. Das `*`-Zeichen ersetzt eine beliebige Sequenz von null oder mehr Zeichen.

   Wenn Sie beispielsweise die Adressmaske `*abc*` eingeben, wird die Zugriffsregel der Webressourcen auf alle Adressen angewendet, in denen die Sequenz `abc` enthalten ist. Beispiel: `http://www.example.com/page_0-9abcdef.html`.

2. Die Zeichenfolge `*.` ermöglicht die Auswahl aller Domänen einer Adresse und stellt damit eine *Domänenmaske* dar. Die Domänenmaske `*.` wird als beliebiger Domänenname, Subdomänenname oder leere Zeichenfolge behandelt.

   Beispiel: Die folgenden Adressen unterliegen der Maske `*.example.com`:

   - `http://pictures.example.com` – wobei die Domänenmaske `*.` auf `pictures` angewendet wird.
   - `http://user.pictures.example.com` – wobei die Domänenmaske `*.` auf `pictures` und `user` angewendet wird.
   - `http://example.com` – wobei die Domänenmaske `*.` als leere Zeichenfolge behandelt wird.

3. Die Sequenz `www.` am Anfang einer Adressmaske wird als Sequenz `*` interpretiert..

   Beispiel: Die Adressmaske `www.example.com` wird als `*.example.com` interpretiert. Die Maske deckt auch die Adressen `www2.example.com` und `www.pictures.example.com` ab.

4. Wenn eine Adressmaske nicht mit dem Zeichen `*` beginnt, entspricht der Inhalt der Adressmaske demselben Inhalt mit dem Präfix `*.`.

5. Wenn eine Adressmaske mit einem anderen Zeichen als `/` oder `*` endet, entspricht der Inhalt der Adressmaske demselben Inhalt mit dem Postfix `/*`.

   Beispiel: Die Adressmaske `http://www.example.com` deckt die Adressen der Form `http://www.example.com/abc` ab, wobei `a`, `b`, `c` beliebige Zeichen sein können.

6. Wenn eine Adressmaske mit einem `/`-Zeichen endet, entspricht der Inhalt der Adressmaske demselben Inhalt mit dem Postfix `/*`.

7. Die Zeichenfolge `/*` am Ende der Adressmaske wird als `/*` oder als leere Zeichenfolge behandelt.

8. Die Prüfung der Adressen von Webressourcen nach Adressmasken erfolgt unter Berücksichtigung des Schemas (http oder https):

   - Wenn in der Adressmaske kein Netzwerkprotokoll angegeben ist, fällt eine Adresse mit einem beliebigen Netzwerkprotokoll unter die Adressmaske.

     Beispiel: Die Adressmaske `example.com` deckt die Adressen `http://example.com` und `https://example.com` ab.

   - Wenn in der Adressmaske ein Netzwerkprotokoll angegeben ist, werden von der Adressmaske nur Adressen mit demselben Netzwerkprotokoll, wie es in der Adressmaske enthalten ist, abgedeckt.

     Beispiel: Die Adressmaske `http://*.example.com` deckt die Adresse `http://www.example.com` ab, aber nicht die Adresse `https://www.example.com`.

9. Eine mit doppelten Anführungszeichen umschlossene Adressmaske wird ohne Berücksichtigung weiterer Ersetzungen behandelt, mit Ausnahme des `*`-Zeichens, wenn es ursprünglich in der Adressmaske enthalten war. Für Adressmasken, die von doppelten Anführungszeichen umschlossen sind, werden die Regeln 5 und 7 nicht angewendet (siehe Beispiele 14 – 18 in der unteren Tabelle).

10. Beim Vergleich mit einer Adressmaske für Webressourcen werden Benutzername, Passwort und Verbindungsport sowie die Groß- und Kleinschreibung nicht berücksichtigt.

Beispiele zur Anwendung der Regeln für die Erstellung von Adressmasken

Nr.	Adressmaske	Geprüfte Adresse einer Webressource	Entspricht die geprüfte Adresse der Adressmaske?	Kommentar
1	*.example.com	http://www.123example.com	Nein	Siehe Regel 1
2	*.example.com	http://www.123.example.com	Ja	Siehe Regel 2
3	*example.com	http://www.123example.com	Ja	Siehe Regel 1
4	*example.com	http://www.123.example.com	Ja	Siehe Regel 1
5	http://www.*.example.com	http://www.123example.com	Nein	Siehe Regel 1
6	www.example.com	http://www.example.com	Ja	Siehe Regeln 3, 2, 1
7	www.example.com	https://www.example.com	Ja	Siehe Regeln 3, 2, 1
8	http://www.*.example.com	http://123.example.com	Ja	Siehe Regeln 3, 4, 1
9	www.example.com	http://www.example.com/abc	Ja	Siehe Regeln 3, 5, 1
10	example.com	http://www.example.com	Ja	Siehe Regeln 3, 1
11	http://example.com/	http://example.com/abc	Ja	Siehe Regel 2
12	http://example.com/*	http://example.com	Ja	Siehe Regel 7
13	http://example.com	https://example.com	Nein	Siehe Regel 8
14	"example.com"	http://www.example.com	Nein	Siehe Regel 9
15	"http://www.example.com"	http://www.example.com/abc	Nein	Siehe Regel 9
16	"*.example.com"	http://www.example.com	Ja	Siehe Regeln 1, 9
17	"http://www.example.com/*"	http://www.example.com/abc	Ja	Siehe Regeln 1, 9
18	"www.example.com"	http://www.example.com; https://www.example.com	Ja	Siehe Regeln 9, 8
19	www.example.com/abc/123	http://www.example.com/abc	Nein	Die Adressmaske enthält mehr Informationen als die Adresse der Webressource.

Überwachung der Systemintegrität

Mit Kaspersky Endpoint Security können Sie die Integrität des Betriebssystems des geschützten Geräts in Echtzeit und auf Befehl überwachen.

- Mit der Komponente *Überwachung der Systemintegrität* können Sie Änderungen in Dateien und Verzeichnissen, die Sie in den Komponenteneinstellungen in den Überwachungsbereich aufgenommen haben, in Echtzeit überwachen. Sie können Änderungen an Dateien überwachen, die eventuell auf eine Verletzung der Sicherheit auf dem geschützten Gerät hindeuten.

- Mithilfe von Aufgaben zur *Prüfung der Systemintegrität* können Sie Dateien und Verzeichnisse, die Sie in den Überwachungsbereich aufgenommen haben, auf Änderungen überprüfen, indem Sie den aktuellen Status des überwachten Objekts mit einem zuvor erfassten Status vergleichen.

Um die Überwachung der Systemintegrität nutzen zu können, benötigen Sie eine Lizenz, in der diese Funktionalität enthalten ist.

Diese Funktionalität wird im KESL-Container nicht unterstützt.

Wenn Kaspersky Endpoint Security im Überwachungsbereich Änderungen an Dateien und Verzeichnissen erkennt, generiert es Ereignisse über Änderungen an den Listen zur Objektzugriffskontrolle. Die Komponente "Überwachung der Systemintegrität" übermittelt keine Informationen darüber, welche Änderungen genau vorgenommen wurden. Die Aufgabe *Prüfung der Systemintegrität* übermittelt Informationen über geänderte Attribute sowie verschobene Dateien und Verzeichnisse.

Überwachung der Systemintegrität in Echtzeit

Mit der Komponente "Überwachung der Systemintegrität" wird jede Änderung an einem Objekt im Überwachungsbereich registriert, indem Dateioperationen in Echtzeit abgefangen werden.

Während der Ausführung der Komponente "Überwachung der Systemintegrität" überwacht die App Änderungen der folgenden Dateieinstellungen:

- Inhalt (write (), truncate (), etc.)
- Metadaten (Besitzrechte (chmod/chown))
- Zeitstempel (utimensat)
- erweiterte Attribute (setxattr) und andere

Die Prüfsumme der Datei wird nicht berechnet.

Aufgrund der technischen Beschränkungen des Betriebssystems Linux kann die App nicht erkennen, welcher Benutzer oder Prozess die Änderungen an einer Datei durchgeführt hat.

Die Überwachung der System-Integrität ist standardmäßig deaktiviert. Sie können die Überwachung der Systemintegrität aktivieren und deaktivieren sowie die Ausführungseinstellungen der Komponente konfigurieren:

- Konfigurieren Sie Überwachungsbereiche zur Überwachung der Systemintegrität. Die App überwacht Dateioperationen in Überwachungsbereichen, die in den Einstellungen der Komponente "Überwachung der Systemintegrität" angegeben sind. Zur Ausführung der Komponente müssen Sie mindestens einen Überwachungsbereich angeben. Standardmäßig ist der Überwachungsbereich *Interne Programmobjekte von Kaspersky* (/opt/kaspersky/kesl/) angegeben.

  Sie können mehrere Überwachungsbereiche angeben. Sie können den Überwachungsbereich im Echtzeitmodus ändern.

  Die App führt keine Überwachung von Dateiänderungen (Attribute und Inhalt) mit harten Links durch, die sich nicht in einem Überwachungsbereich befinden.

- Sie können den Ausschluss von Objekten von der Überwachung anhand einer Namensmaske konfigurieren.

- Konfigurieren Sie Ausschlussbereiche zur Überwachung der Systemintegrität. Ausschlüsse werden für jeden einzelnen Überwachungsbereich angegeben und funktionieren nur für den angegebenen Bereich. Sie können mehrere Ausschlüsse vom Überwachungsbereich angeben.

  Ein Ausschluss hat eine höhere Priorität als der Überwachungsbereich; das ausgeschlossene Objekt wird nicht überwacht, auch wenn es sich im Überwachungsbereich befindet. Wenn ein Überwachungsbereich auf einer niedrigeren Ebene als dem im Ausschluss angegebenen Verzeichnis festgelegt ist, überwacht die App diesen Überwachungsbereich während der Überwachung der Systemintegrität nicht.

Wenn ein Verzeichnis zum Überwachungs- oder Ausschlussbereich hinzugefügt wird, prüft die App nicht, ob das angegebene Verzeichnis existiert.

Überwachung der Systemintegrität in der Web Console konfigurieren

In der Web Console können Sie Einstellungen der Überwachung der Systemintegrität in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen** → **Sicherheitskontrolle** → **Überwachung der Systemintegrität**).

Einstellungen der Komponente "Überwachung der Systemintegrität"

Einstellung	Beschreibung
Überwachung der System-Integrität aktiviert/deaktiviert	Dieser Schalter aktiviert und deaktiviert die Komponente "Überwachung der Systemintegrität". Der Schalter ist standardmäßig deaktiviert.
Überwachungsbereiche	Der Link **Überwachungsbereiche anpassen** öffnet das Fenster Überwachungsbereiche.
Ausschlussbereiche	Der Link **Ausschlussbereiche von der Überwachung anpassen** öffnet das Fenster Überwachungsbereiche.
Ausschlüsse nach Maske	Der Link **Ausschlüsse nach Maske anpassen** öffnet das Fenster Ausschlüsse nach Maske.

Fenster "Überwachungsbereiche"

Die Tabelle enthält die Überwachungsbereiche der Komponente "Überwachung der System-Integrität". Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle den Überwachungsbereich **Interne Programmobjekte von Kaspersky** (/opt/kaspersky/kesl/).

Einstellungen des Überwachungsbereichs der Komponente "Überwachung der System-Integrität"

Einstellung	Beschreibung
Name des Bereichs	Name des Überwachungsbereichs.
Pfad	Pfad zum geschützten Verzeichnis.
Status	Der Status gibt an, ob die App diesen Bereich während ihrer Ausführung untersucht.

Sie können Elemente in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.

Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Liste angeben sind. Um bei Bedarf für das Unterverzeichnis andere Sicherheitseinstellungen festzulegen als für das übergeordnete Verzeichnis, platzieren Sie erforderlichenfalls das Unterverzeichnis in der Liste über dem übergeordneten Verzeichnis.

Fenster zum Hinzufügen des Überwachungsbereichs

In diesem Fenster können Sie Überwachungsbereiche für die Komponente "Überwachung der System-Integrität" hinzufügen und bearbeiten.

Einstellungen des Überwachungsbereichs

Einstellung	Beschreibung
Name des Bereichs	Eingabefeld für den Namen des Überwachungsbereichs. Dieser Name wird in der Tabelle im Fenster **Überwachungsbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.

Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung dieses Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, überwacht die App diesen Bereich während der Ausführung. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich von der App während der Ausführung nicht überwacht. Sie können diesen Bereich zu einem späteren Zeitpunkt zu den Betriebseinstellungen der Komponente hinzufügen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Eingabefeld für den Pfad des lokalen Verzeichnisses, das in den Überwachungsbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken verwenden. Das Feld darf nicht leer sein. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardmäßige Pfadangabe **/** – Die App untersucht alle Verzeichnisse des lokalen Dateisystems.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der App während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske ***** (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster. Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Ausschlussbereiche"

Die Tabelle enthält die Ausschlussbereiche der Komponente "Überwachung der System-Integrität". Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.

Einstellungen des Bereichs mit Ausschlüsse von der Überwachung

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Pfad zum Verzeichnis, das von der Überwachung ausgenommen ist.
Status	Der Status gibt an, ob die App diesen Bereich während der Ausführung der Komponente von der Überwachung ausschließt.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster zum Hinzufügen des Ausschlussbereichs

In diesem Fenster können Sie einen Bereich mit Ausschlüsse von der Überwachung für die Komponente "Überwachung der System-Integrität" hinzufügen und bearbeiten.

Einstellungen des Bereichs mit Ausschlüsse von der Überwachung

Einstellung	Beschreibung
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster **Ausschlussbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss des Bereichs von der Überwachung während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während der Ausführung der Komponente von der Überwachung aus. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich von der App während der Ausführung der Komponente überwacht. Im Folgenden können Sie diesen Bereich von der Überwachung ausschließen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.

Dateisystem, Zugriffsprotokoll und Pfad	Eingabefeld für den Pfad des lokalen Verzeichnisses, das in den Ausschlussbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken verwenden. Das Feld darf nicht leer sein. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Als Pfad ist standardmäßig **/** angegeben: Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Überwachung ausgeschlossen werden. Standardmäßig enthält die Liste die Maske ***** (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster. Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Ausschlüsse nach Maske"

Sie können den Ausschluss von Objekten von der Überwachung anhand einer Namensmaske konfigurieren. Die App untersucht keine Dateien, deren Namen die angegebenen Masken enthalten. Standardmäßig ist die Liste mit Masken leer.

Sie können Masken hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Überwachung der Systemintegrität in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie Einstellungen zur Überwachung der Systemintegrität in den Richtlinieneinstellungen konfigurieren (**Sicherheitskontrolle → Überwachung der Systemintegrität**).

Einstellungen der Komponente "Überwachung der Systemintegrität"

Einstellung	Beschreibung
Überwachung der System-Integrität aktivieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Überwachung der System-Integrität. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Überwachungsbereiche	Diese Parametergruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Untersuchungsbereiche** öffnet.
Ausschlüsse von der Überwachung	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausschlussbereiche** öffnet.
Ausschlüsse nach Maske	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausschlüsse nach Maske** öffnet.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält die Überwachungsbereiche für die Komponente "Überwachung der System-Integrität". Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle nur den Überwachungsbereich **Interne Kaspersky-Objekte** (/opt/kaspersky/kesl/).

Einstellungen des Überwachungsbereichs

Einstellung	Beschreibung
Name des Bereichs	Name des Überwachungsbereichs.
Pfad	Pfad zum geschützten Verzeichnis.
Status	Der Status gibt an, ob die App diesen Bereich während ihrer Ausführung untersucht.

Sie können Elemente in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.

Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Liste angeben sind. Um bei Bedarf für das Unterverzeichnis andere Sicherheitseinstellungen festzulegen als für das übergeordnete Verzeichnis, platzieren Sie erforderlichenfalls das Unterverzeichnis in der Liste über dem übergeordneten Verzeichnis.

Fenster "<Neuer Untersuchungsbereich>"

In diesem Fenster können Sie Überwachungsbereiche für die Komponente "Überwachung der System-Integrität" hinzufügen und bearbeiten.

Einstellungen des Überwachungsbereichs

Einstellung	Beschreibung
Name des Untersuchungsbereichs	Eingabefeld für den Namen des Überwachungsbereichs. Dieser Name wird in der Tabelle im Fenster **Untersuchungsbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.

Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung dieses Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, überwacht die App diesen Bereich während der Ausführung. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich von der App während der Ausführung nicht überwacht. Sie können diesen Bereich zu einem späteren Zeitpunkt zu den Betriebseinstellungen der Komponente hinzufügen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Eingabefeld für den Pfad des lokalen Verzeichnisses, das in den Überwachungsbereich aufgenommen werden soll. Das Feld darf nicht leer sein. Standardmäßig ist der Pfad "/opt/kaspersky/kesl" angegeben.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der App während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster. Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Ausschlussbereiche"

Die Tabelle enthält die Ausschlussbereiche der Komponente "Überwachung der System-Integrität". Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.

Einstellungen des Bereichs mit Ausschlüsse von der Überwachung

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Pfad zum Verzeichnis, das von der Überwachung ausgenommen ist.
Status	Der Status gibt an, ob die App diesen Bereich während der Ausführung der Komponente von der Überwachung ausschließt.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster <Name des Ausschlussbereichs>

In diesem Fenster können Sie einen Bereich mit Ausschlüsse von der Überwachung für die Komponente "Überwachung der System-Integrität" hinzufügen und bearbeiten.

Einstellungen des Bereichs mit Ausschlüsse von der Überwachung

Einstellung	Beschreibung
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster **Ausschlussbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss des Bereichs von der Überwachung während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während der Ausführung der Komponente von der Überwachung aus. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich von der App während der Ausführung der Komponente überwacht. Im Folgenden können Sie diesen Bereich von der Überwachung ausschließen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Eingabefeld für den Pfad des lokalen Verzeichnisses, das in den Ausschlussbereich aufgenommen werden soll. Das Feld darf nicht leer sein. Als Pfad ist standardmäßig **/** angegeben: Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Überwachung ausgeschlossen werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Maske"

Sie können den Ausschluss von Objekten von der Überwachung anhand einer Namensmaske konfigurieren. Die App untersucht keine Dateien, deren Namen die angegebenen Masken enthalten. Standardmäßig ist die Liste mit Masken leer.

Sie können Masken hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Überwachung der Systemintegrität über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Überwachung der Systemintegrität in Echtzeit mithilfe der vordefinierten Aufgabe "Überwachung der Systemintegrität" (*System_Integrity_Monitoring*) verwalten. Aufgabentyp – *OAFIM*.

Die Aufgabe "Überwachung der Systemintegrität" wird standardmäßig nicht gestartet. Sie können diese Aufgabe manuell starten und anhalten.

Sie können die Einstellungen der Überwachung der Systemintegrität auf dem Gerät konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zur Überwachung der Systemintegrität ändern.

Einstellungen der Aufgabe zur Überwachung der System-Integrität bei Zugriff

Einstellung	Beschreibung	Werte
`UseExcludeMasks`	Aktiviert den Ausschluss von Objekten aus dem Überwachungsbereich, die in der Einstellung `ExcludeThreats.item_#` angegeben sind. Diese Einstellung funktioniert nur, wenn die Einstellung `ExcludeMasks.item_#` angegeben ist.	`Yes` – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, aus dem Überwachungsbereich ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht aus dem Überwachungsbereich ausschließen.
`ExcludeMasks.item_#`	Ausschluss von der Überwachung von Objekten nach Name oder Maske. Mit dieser Einstellung können Sie eine einzelne Datei anhand des Namens oder mehrere Dateien anhand von Masken im Shell-Format aus dem angegebenen Untersuchungsbereich ausschließen. Bevor Sie den Wert dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseExcludeMasks` aktiviert ist. Sie können mehrere Masken angeben, jede Maske muss in einer neuen Zeile mit einem neuen Index angegeben werden.	Der Standardwert ist nicht angegeben.
Der Abschnitt **[ScanScope.item_#]** enthält die von der Aufgabe zur Überwachung der System-Integrität zu überwachenden Bereiche. Für die Aufgabe muss zumindest ein Überwachungsbereich festgelegt sein. Sie können mehrere Abschnitte [ScanScope.item_#] in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge. Der Abschnitt [ScanScope.item_#] enthält folgende Einstellungen:		
`AreaDesc`	Beschreibung des Überwachungsbereichs mit zusätzlichen Informationen über den Überwachungsbereich.	Der Standardwert ist nicht angegeben.
`UseScanArea`	Aktiviert die Überwachung des angegebenen Bereichs.	`Yes` (Standardwert) – Den angegebenen Bereich überwachen. `No` – Den angegebenen Bereich nicht überwachen.
`Path`	Pfad zum Verzeichnis, das überwacht werden soll.	Bei der Angabe des Pfades können Sie Masken verwenden.

		Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardwert: /opt/kaspersky/kesl/
`AreaMask.item_#`	Einschränkung des Überwachungsbereichs. Im Überwachungsbereich untersucht die App nur Objekte, die mit Masken im Shell-Format angegeben wurden.	Standardwert: * (alle Objekte werden überwacht)

	Sie können mehrere Elemente vom Typ `AreaMask.item_#` in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge.	
Der Abschnitt **[ExcludedFromScanScope.item_#]** enthält Objekte, die von allen Abschnitten [ScanScope.item_#] ausgeschlossen werden sollen. Sie können mehrere Abschnitte [ExcludedFromScanScope.item_#] in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge. Der Abschnitt [ExcludedFromScanScope.item_#] enthält folgende Einstellungen:		
`AreaDesc`	Beschreibung des Ausschlussbereichs von der Überwachung mit zusätzlichen Informationen über den Ausschlussbereich von der Überwachung.	Der Standardwert ist nicht angegeben.
`UseScanArea`	Schließt den angegebenen Bereich von der Überwachung aus.	`Yes` (Standardwert) – Den angegebenen Bereich aus der Überwachung ausschließen. `No` – Den angegebenen Bereich nicht aus der Überwachung ausschließen.
`Path`	Pfad zum Verzeichnis mit Objekten, die von der Überwachung ausgeschlossen sind.	Bei der Angabe des Pfades können Sie Masken verwenden.

		Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Der Standardwert ist nicht angegeben.
`AreaMask.item_#`	Einschränkung des Ausschlussbereichs von der Überwachung. Im Ausschlussbereich von der Überwachung schließt die App nur Objekte aus, die mittels Masken im Shell-Format angegeben wurden.	Standardwert: * (alle Objekte von der Überwachung ausschließen)

	Sie können mehrere Elemente vom Typ `AreaMask.item_#` in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge.	

Überwachung der System-Integrität

Während der Ausführung der Aufgabe *Prüfung der Systemintegrität* werden Änderungen in jedem Objekt ermittelt, indem der aktuelle Status des überwachten Objekts mit dem Originalstatus verglichen wird. Vergleiche können anhand der folgenden Kriterien durchgeführt werden:

- Datei-Hash
- Zeitpunkt der Dateiänderung
- Dateigröße

Der Originalstatus der überwachten Objekte wird als *Baseline* aufgezeichnet. Die Baseline enthält Pfade zu überwachten Objekten und deren Metadaten.

Die Baseline kann persönliche Daten enthalten.

Die Baseline wird während der ersten Ausführung der Aufgabe zur Prüfung der Systemintegrität auf dem Gerät erstellt. Wenn Sie mehrere Aufgaben zur Prüfung der Systemintegrität erstellt haben, wird für jede Aufgabe eine separate Baseline erstellt. Die Aufgabe wird nur ausgeführt, wenn die Baseline Informationen zu Objekten enthält, die zum für die Aufgabe konfigurierten Überwachungsbereich gehören. Wenn die Baseline nicht dem Überwachungsbereich entspricht, erstellt die App Kaspersky Endpoint Security ein Ereignis über die Verletzung der System-Integrität.

Eine Baseline wird dann neu erstellt, wenn die Einstellungen einer Aufgabe geändert werden (z. B. wenn ein neuer Überwachungsbereich hinzugefügt wurde).

Die App erstellt Speicher für Baselines auf dem geschützten Gerät. Standardmäßig befindet sich der Speicher für Baselines unter /var/opt/kaspersky/kesl/private/fim.db. Für den Zugriff auf die Datenbank mit Baselines sind Root-Rechte erforderlich.

Sie können eine Baseline löschen, indem Sie die entsprechende Aufgabe zur Prüfung der Systemintegrität löschen.

Sie können die Prüfung der Systemintegrität auf Befehl durchführen und Einstellungen für die Prüfung konfigurieren:

- Aktivieren und deaktivieren Sie die Aktualisierung der Baseline jedes Mal nach Abschluss der Aufgabe zur Prüfung der Systemintegrität.
- Wählen Sie die Kriterien aus, anhand derer der aktuelle Status der überwachten Datei mit dem Originalstatus verglichen wird: Verwenden Sie den Hash und den Zeitpunkt der Dateiänderung oder nur die Dateigröße.
- Konfigurieren Sie Überwachungsbereiche zur Prüfung der Systemintegrität.
- Konfigurieren Sie Bereiche, die von der Prüfung der Systemintegrität ausgeschlossen werden sollen. Sie können Pfade zu ausgeschlossenen Dateien und Verzeichnissen angeben und einzelne Objekte anhand der Namensmaske ausschließen.

Prüfung der Systemintegrität in der Web Console

In der Web Console können Sie mithilfe der Aufgabe *Prüfung der Systemintegrität* Prüfungen der Systemintegrität durchführen.

Sie können Benutzeraufgaben für die Prüfung der Systemintegrität erstellen und starten. Sie können die Untersuchungseinstellungen konfigurieren, indem Sie die Aufgabeneinstellungen ändern.

Einstellungen der Aufgabe zur Untersuchung der System-Integrität

Einstellung	Beschreibung
Baseline bei jedem Aufgabenstart aktualisieren	Dieses Kontrollkästchen aktiviert oder deaktiviert die Neuerstellung der Baseline bei jedem Start der Aufgabe *Prüfung der Systemintegrität*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
SHA256-Hash für die Untersuchung verwenden	Dieses Kontrollkästchen aktiviert oder deaktiviert die Verwendung des Datei-Hash als Kriterium für den Vergleich des aktuellen Status der Datei mit dem Originalstatus. Wenn das Kontrollkästchen deaktiviert ist, vergleicht die App nur die Dateigröße (wenn sich die Dateigröße nicht geändert hat, wird der Zeitpunkt der Änderung nicht als kritischer Parameter betrachtet). Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Verzeichnisse in Überwachungsbereichen verfolgen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Untersuchung von Verzeichnissen während der Prüfung der Systemintegrität. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Zeitpunkt des letzten Zugriffs auf Dateien überwachen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Überwachung des Zeitpunkts des Dateizugriffs während der Prüfung der Systemintegrität. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Überwachungsbereiche	Eine Tabelle mit Überwachungsbereichen, die von der Aufgabe untersucht werden sollen. Standardmäßig enthält die Tabelle den Überwachungsbereich **Interne Programmobjekte von Kaspersky** (/opt/kaspersky/kesl/). Sie können Überwachungsbereiche in der Tabelle hinzufügen, konfigurieren, löschen, nach oben verschieben und nach unten verschieben. Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten. Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren. Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Tabelle der Untersuchungsbereiche angeben sind. Wenn Sie für das Unterverzeichnis andere Sicherheitseinstellungen festlegen möchten als für das übergeordnete Verzeichnis, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Wenn Sie auf die Schaltfläche **Löschen** klicken, wird der ausgewählte Bereich von der Untersuchung ausgeschlossen.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Untersuchungsbereich ausgewählt ist.

Ein Klick auf den Namen des Untersuchungsbereichs öffnet das Fenster **<Name des Untersuchungsbereichs>**. In diesem Fenster können Sie die Einstellungen des ausgewählten Untersuchungsbereichs ändern.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **<Neuer Untersuchungsbereich>**. In diesem Fenster können Sie einen neuen Untersuchungsbereich festlegen.

Fenster zum Hinzufügen des Untersuchungsbereichs

In diesem Fenster können Sie den Überwachungsbereich für die Aufgabe zur Überwachung der System-Integrität hinzufügen und bearbeiten.

Einstellungen des Überwachungsbereichs

Einstellung	Beschreibung
Name des Bereichs	Eingabefeld für den Namen des Überwachungsbereichs. Dieser Name wird in der Tabelle im Abschnitt **Untersuchungseinstellungen** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung dieses Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, überwacht die App diesen Bereich während der Ausführung. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich von der App während der Ausführung nicht überwacht. Sie können diesen Bereich zu einem späteren Zeitpunkt zu den Betriebseinstellungen der Komponente hinzufügen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.

Dateisystem, Zugriffsprotokoll und Pfad	Eingabefeld für den Pfad des lokalen Verzeichnisses, das in den Überwachungsbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld darf nicht leer sein. Standardmäßige Pfadangabe **/** – Die App untersucht alle Verzeichnisse des lokalen Dateisystems.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der App während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster. Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Abschnitt "Ausschlussbereiche"

Im Abschnitt **Ausschlussbereiche** können Sie die Ausschlussbereiche von der Prüfung und Ausschlüsse nach Maske für die Aufgabe zur Überwachung der System-Integrität konfigurieren.

Fenster "Ausschlussbereiche"

Die Tabelle enthält die Ausschlussbereiche der Komponente "Prüfung der System-Integrität". Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.

Einstellungen des Bereichs mit Ausschlüsse von der Überwachung

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Pfad zum Verzeichnis, das von der Überwachung ausgenommen ist.
Status	Der Status gibt an, ob die App diesen Bereich während der Ausführung der Aufgabe von der Überwachung ausschließt.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster zum Hinzufügen des Ausschlussbereichs

In diesem Fenster können Sie einen Bereich mit Ausschlüssen von der Überwachung für die Aufgabe zur Prüfung der System-Integrität hinzufügen und bearbeiten.

Einstellungen des Bereichs mit Ausschlüsse von der Überwachung

Einstellung	Beschreibung
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster **Ausschlussbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss des Bereichs von der Überwachung während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während der Ausführung der Aufgabe von der Überwachung aus. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich von der App während der Ausführung der Aufgabe überwacht. Im Folgenden können Sie diesen Bereich von der Überwachung ausschließen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll	Eingabefeld für den Pfad des lokalen Verzeichnisses, das in den Ausschlussbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken

und Pfad	verwenden. Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld darf nicht leer sein. Als Pfad ist standardmäßig **/** angegeben: Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Überwachung ausgeschlossen werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster. Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "Ausschlüsse nach Maske"

Sie können den Ausschluss von Objekten von der Überwachung anhand einer Namensmaske konfigurieren. Die App untersucht keine Dateien, deren Namen die angegebenen Masken enthalten. Standardmäßig ist die Liste mit Masken leer.

Sie können Masken hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Prüfung der Systemintegrität in der Verwaltungskonsole

In der Verwaltungskonsole können Sie mithilfe der Aufgabe *Prüfung der Systemintegrität* Prüfungen der Systemintegrität durchführen.

Sie können Benutzeraufgaben für die Prüfung der Systemintegrität erstellen und starten. Sie können die Untersuchungseinstellungen konfigurieren, indem Sie die Aufgabeneinstellungen ändern.

Im Abschnitt **Einstellungen** in den Eigenschaften der Aufgabe "Prüfung der Systemintegrität" können Sie die in der folgenden Tabelle aufgeführten Einstellungen konfigurieren.

Einstellungen der Aufgabe zur Untersuchung der System-Integrität

Einstellung	Beschreibung
Baseline bei jedem Aufgabenstart aktualisieren	Dieses Kontrollkästchen aktiviert oder deaktiviert die Neuerstellung der Baseline bei jedem Start der Aufgabe Prüfung der Systemintegrität. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Hash (SHA256) für die Untersuchung verwenden	Dieses Kontrollkästchen aktiviert oder deaktiviert die Verwendung des Datei-Hash als Kriterium für den Vergleich des aktuellen Status der Datei mit dem Originalstatus. Wenn das Kontrollkästchen deaktiviert ist, vergleicht die App nur die Dateigröße (wenn sich die Dateigröße nicht geändert hat, wird der Zeitpunkt der Änderung nicht als kritischer Parameter betrachtet). Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Verzeichnisse in Überwachungsbereichen verfolgen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Untersuchung von Verzeichnissen in den angegebenen Überwachungsbereichen während der Prüfung der Systemintegrität. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Zeitpunkt des letzten Zugriffs auf Dateien überwachen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Überwachung des Zeitpunkts des Dateizugriffs während der Prüfung der Systemintegrität. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Überwachungsbereiche	Diese Parametergruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Untersuchungsbereiche** öffnet.

Im Abschnitt **Ausschlussbereiche** in den Eigenschaften der Aufgabe "Prüfung der Systemintegrität" können Sie Ausschlüsse vom Überwachungsbereich und Ausschlüsse nach Maske konfigurieren.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält die Überwachungsbereiche der Aufgabe zur Prüfung der System-Integrität. Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle nur den Überwachungsbereich **Interne Kaspersky-Objekte** (/opt/kaspersky/kesl/).

Einstellungen des Überwachungsbereichs

Einstellung	Beschreibung
Name des Bereichs	Name des Überwachungsbereichs.
Pfad	Pfad zum geschützten Verzeichnis.
Status	Der Status gibt an, ob die App diesen Bereich während ihrer Ausführung untersucht.

Sie können Elemente in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.

Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Kaspersky Endpoint Security untersucht Objekte in den angegebenen Bereichen in der Reihenfolge, in der sie in der Liste angeben sind. Um bei Bedarf für das Unterverzeichnis andere Sicherheitseinstellungen festzulegen als für das übergeordnete Verzeichnis, platzieren Sie erforderlichenfalls das Unterverzeichnis in der Liste über dem übergeordneten Verzeichnis.

Fenster "<Neuer Untersuchungsbereich>"

In diesem Fenster können Sie den Überwachungsbereich für die Aufgabe zur Prüfung der System-Integrität hinzufügen und bearbeiten.

Einstellungen des Überwachungsbereichs

Einstellung	Beschreibung
Name des Untersuchungsbereichs	Eingabefeld für den Namen des Überwachungsbereichs. Dieser Name wird in der Tabelle im Fenster **Untersuchungsbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung dieses Bereichs während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, überwacht die App diesen Bereich während der Ausführung. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich von der App während der Ausführung nicht überwacht. Sie können diesen Bereich zu einem späteren Zeitpunkt zu den Betriebseinstellungen der Komponente hinzufügen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Eingabefeld für den Pfad des lokalen Verzeichnisses, das in den Überwachungsbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld darf nicht leer sein. Standardmäßig ist der Pfad "/opt/kaspersky/kesl" angegeben.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der App während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Abschnitt "Ausschlussbereiche"

Einstellungen der Ausschlüsse von der Untersuchung

Einstellungsgruppe	Beschreibung
Ausschlüsse von der Überwachung	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster Ausschlussbereiche öffnet. In diesem Fenster können Sie eine Liste mit Bereichen festlegen, die von der Überwachung ausgeschlossen werden sollen.
Ausschlüsse nach Maske	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster Ausschlüsse nach Maske öffnet. In diesem Fenster können Sie die Ausschlüsse von Objekten aus der Überwachung anhand einer Namensmaske konfigurieren.

Fenster "Ausschlussbereiche"

Die Tabelle enthält die Ausschlussbereiche für die Aufgabe zur Prüfung der System-Integrität. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.

Einstellungen des Ausschlussbereiche für die Aufgabe zur Prüfung der System-Integrität

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status gibt an, ob die App diesen Bereich während der Ausführung der Aufgabe von der Überprüfung ausschließt.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Fenster "<Neuer Ausschlussbereich>"

In diesem Fenster können Sie einen Bereich mit Ausschlüssen von der Überwachung für die Aufgabe zur Prüfung der System-Integrität hinzufügen und bearbeiten.

Einstellungen des Bereichs mit Ausschlüsse von der Überwachung

Einstellung	Beschreibung
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster **Ausschlussbereiche** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss des Bereichs von der Überwachung während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während der Ausführung der Aufgabe von der Überwachung aus. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich von der App während der Ausführung der Aufgabe überwacht. Im Folgenden können Sie diesen Bereich von der Überwachung ausschließen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	Eingabefeld für den Pfad des lokalen Verzeichnisses, das in den Ausschlussbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie Masken verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld darf nicht leer sein. Als Pfad ist standardmäßig **/** angegeben: Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus.

Masken	Diese Liste enthält die Namensmasken von Objekten, die von der App von der Überwachung ausgeschlossen werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen. Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle. Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist. Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster. Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll. Beispiele: Die Maske `*.txt` bezieht sich auf alle Textdateien. Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Fenster "Ausschlüsse nach Maske"

Sie können den Ausschluss von Objekten von der Überwachung anhand einer Namensmaske konfigurieren. Die App untersucht keine Dateien, deren Namen die angegebenen Masken enthalten. Standardmäßig ist die Liste mit Masken leer.

Sie können Masken hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.

Ein Klick auf die Schaltfläche **Hinzufügen** öffnet das Fenster **Objektmaske**. In diesem Fenster können Sie im Feld **Geben Sie die Objektmaske an** die Vorlage für die Namen der Dateien festlegen, die Kaspersky Endpoint Security aus der Untersuchung ausschließen soll.

Beispiele:
Die Maske `*.txt` bezieht sich auf alle Textdateien.
Die Maske `*_my_file_??.html` bezieht sich auf html-Dateien, die beliebig beginnen und mit `_my_file_` gefolgt von zwei beliebigen Zeichen enden (z. B. 2020_my_file_09.html).

Prüfung der Systemintegrität über die Befehlszeile

Über die Befehlszeile können Sie Prüfungen der Systemintegrität auf dem Gerät durchführen, indem Sie Benutzeraufgaben für die *Prüfung der Systemintegrität* (Aufgaben vom Typ *ODFIM*) verwenden.

Sie können Benutzeraufgaben manuell starten, beenden, anhalten und fortsetzen und den Zeitplan für den Aufgabenstart konfigurieren. Sie können die Einstellungen für die Prüfung der Systemintegrität konfigurieren, indem Sie die Einstellungen für diese Aufgaben ändern.

Einstellungen der Aufgabe zur Untersuchung der System-Integrität

Einstellung	Beschreibung	Werte
`RebuildBaseline`	Aktivieren Sie die Neuerstellung der Baseline nach Abschluss der Aufgabe *Prüfung der Systemintegrität*.	`Ja` – Aktualisiert die Baseline jedes Mal nach Abschluss der Aufgabe *Prüfung der Systemintegrität*. `Nein` (Standard) – Die Baseline wird nicht jedes Mal nach Abschluss der Aufgabe *Prüfung der Systemintegrität* aktualisiert.
`CheckFileHash`	Verwenden Sie den Datei-Hash (SH256) als Kriterium, anhand dessen der aktuelle Status der kontrollierten Datei mit dem Originalstatus verglichen wird.	`Yes` – Hash untersuchen. `No` (Standardwert) – Hash-Prüfung deaktivieren. Wenn die Prüfung deaktiviert ist, vergleicht die App nur die Dateigröße (wenn sich die Dateigröße nicht geändert hat, wird der Zeitpunkt der Änderung nicht als kritischer Parameter betrachtet).
`TrackDirectoryChanges`	Aktiviert die Verzeichnisüberwachung.	`Yes` – Verzeichnisse während der Prüfung der Systemintegrität überwachen. `No` (Standardwert) – Verzeichnisse nicht überwachen.

`TrackLastAccessTime`	Aktiviert die Prüfung des Zeitpunkts des letzten Dateizugriffs In Linux-Betriebssystemen ist die der Parameter `noatime`.	`Yes` – Zeitpunkt des letzten Dateizugriffs prüfen. `No` (Standardwert) – Zeitpunkt des letzten Dateizugriffs nicht prüfen.
`UseExcludeMasks`	Aktiviert den Ausschluss von Objekten aus dem Überwachungsbereich, die in der Einstellung `ExcludeMasks.item_#` angegeben sind. Diese Einstellung funktioniert nur, wenn die Einstellung `ExcludeMasks.item_#` angegeben ist.	`Yes` – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, aus dem Überwachungsbereich ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht aus dem Überwachungsbereich ausschließen.
`ExcludeMasks.item_#`	Ausschluss von der Überwachung von Objekten nach Name oder Maske. Mit dieser Einstellung können Sie eine einzelne Datei anhand des Namens oder mehrere Dateien anhand von Masken im Shell-Format aus dem angegebenen Untersuchungsbereich ausschließen. Bevor Sie den Wert dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseExcludeMasks` aktiviert ist. Sie können mehrere Masken angeben, jede Maske muss in einer neuen Zeile mit einem neuen Index angegeben werden.	Der Standardwert ist nicht angegeben.
Der Abschnitt **[ScanScope.item_#]** enthält die von der Aufgabe *Prüfung der Systemintegrität* zu überwachenden Bereiche. Für die Aufgabe muss zumindest ein Überwachungsbereich festgelegt sein. Sie können mehrere Abschnitte [ScanScope.item_#] in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge. Der Abschnitt [ScanScope.item_#] enthält folgende Einstellungen:		
`AreaDesc`	Beschreibung des Überwachungsbereichs mit zusätzlichen Informationen über den Überwachungsbereich.	Der Standardwert ist nicht angegeben.
`UseScanArea`	Aktiviert die Überwachung des angegebenen Bereichs.	`Yes` (Standardwert) – Den angegebenen Bereich überwachen. `No` – Den angegebenen Bereich nicht überwachen.
`Path`	Pfad zum Verzeichnis, das überwacht werden soll.	Bei der Angabe des Pfades können Sie Masken verwenden.

		Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardwert: /opt/kaspersky/kesl/
`AreaMask.item_#`	Einschränkung des Überwachungsbereichs. Im Überwachungsbereich untersucht die App nur Objekte, die mit Masken im Shell-Format angegeben wurden.	Standardwert: * (alle Objekte werden überwacht)

	Sie können mehrere Elemente vom Typ `AreaMask.item_#` in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge.	
Der Abschnitt **[ExcludedFromScanScope.item_#]** enthält Objekte, die aus allen Abschnitten von [ScanScope.item_#] ausgeschlossen werden müssen. Sie können mehrere Abschnitte [ExcludedFromScanScope.item_#] in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge. Der Abschnitt [ExcludedFromScanScope.item_#] enthält folgende Einstellungen:		
`AreaDesc`	Beschreibung des Ausschlussbereichs von der Überwachung mit zusätzlichen Informationen über den Ausschlussbereich von der Überwachung.	Der Standardwert ist nicht angegeben.
`UseScanArea`	Schließt den angegebenen Bereich von der Überwachung aus.	`Yes` (Standardwert) – Den angegebenen Bereich aus der Überwachung ausschließen. `No` – Den angegebenen Bereich nicht aus der Überwachung ausschließen.
`Path`	Pfad zum Verzeichnis mit Objekten, die von der Überwachung ausgeschlossen sind.	Bei der Angabe des Pfades können Sie Masken verwenden.

		Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Der Standardwert ist nicht angegeben.
`AreaMask.item_#`	Einschränkung des Ausschlussbereichs von der Überwachung. Im Ausschlussbereich von der Überwachung schließt die App nur Objekte aus, die mittels Masken im Shell-Format angegeben wurden.	Standardwert: * (alle Objekte von der Überwachung ausschließen)

	Sie können mehrere Elemente vom Typ `AreaMask.item_#` in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge.	

Verhaltensanalyse

Mit der Komponente "Verhaltensanalyse" können Sie schädliche Aktivitäten von Apps im Betriebssystem überwachen. Wenn schädliche Aktivitäten erkannt werden, kann Kaspersky Endpoint Security den Prozess der App, welche die bösartigen Aktivitäten ausführt, beenden.

Diese Funktionalität wird im KESL-Container nicht unterstützt.

Die Komponente "Verhaltensanalyse" wird beim Start von Kaspersky Endpoint Security automatisch mit den Standardeinstellungen aktiviert.

Sie können die Verhaltensanalyse aktivieren und deaktivieren sowie die Ausführungseinstellungen der Komponente konfigurieren:

- Wählen Sie die Aktion aus, die Kaspersky Endpoint Security ausführen soll, wenn im Betriebssystem schädliche Aktivitäten erkannt werden: Benutzer informieren oder App, die schädliche Aktivitäten ausführt, blockieren.
- Schließen Sie Prozessaktivitäten von der Untersuchung aus.

Wenn die Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response aktiviert ist, werden bei der Analyse des Verhaltens von Apps im Betriebssystem keine Ausschlüsse nach Prozess angewendet.

Die Konfiguration des Dienstes "auditd" ist auf dem Betriebssystem SintezM-Client standardmäßig gegen Änderungen gesperrt, d. h. sie befindet sich im Ausführungsmodus `enabled 2`. Damit die Komponente "Verhaltensanalyse" bei einer Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response und Kaspersky Anti Targeted Attack Platform ordnungsgemäß funktioniert, müssen Sie in den Konfigurationsdateien den Ausführungsmodus von auditd in den Modus ohne Sperrung der Konfiguration (d. h. `enabled 1`) ändern und anschließend einen Neustart des Betriebssystems durchführen.

Verhaltensanalyse in der Web Console konfigurieren

In der Web Console können Sie Einstellungen zur Verhaltensanalyse für Apps in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen** → **Erweiterter Schutz** → **Verhaltensanalyse**).

Einstellungen der Komponente "Verhaltensanalyse"

Einstellung	Beschreibung
Verhaltensanalyse aktiviert/deaktiviert	Dieser Schalter aktiviert und deaktiviert die Komponente "Verhaltensanalyse". Der Schalter ist standardmäßig aktiviert.
Aktion, wenn schädliche Aktivitäten erkannt werden	Aktion, die Kaspersky Endpoint Security ausführen soll, wenn schädliche Aktivitäten im Betriebssystem erkannt werden: • **Informieren** Sie den Benutzer. Kaspersky Endpoint Security beendet den Prozess, der schädliche Aktivitäten ausführt, nicht, sondern protokolliert nur das Ereignis eines Funds schädliche Aktivität im Ereignisprotokoll. • App, die eine schädliche Aktivität ausführt **blockieren** (Standardwert). Kaspersky Endpoint Security beendet den Prozess, der schädliche Aktivität ausführt, und trägt Daten über die erkannte schädliche Aktivität in das Ereignisprotokoll ein.

Ausschlüsse nach Prozess	Der Link **Ausschlüsse nach Prozessen anpassen** öffnet das Fenster **Ausschlüsse nach Prozessen**. In diesem Fenster können Sie den Ausschluss der Aktivität von Prozessen aus der Untersuchung konfigurieren.

Fenster "Ausschlüsse nach Prozess"

Die Tabelle enthält Ausschlussbereiche nach Prozessen. Mit dem Ausschlussbereich nach Prozessen können Sie den Ausschluss der Aktivität des angegebenen Prozesses und der vom angegebenen Prozess geänderten Dateien konfigurieren. Standardmäßig ist die Tabelle leer.

Wenn die Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response aktiviert ist, werden keine Ausschlüsse nach Prozess angewendet.

Einstellungen des Ausschlussbereichs nach Prozessen

Einstellung	Beschreibung
Vertrauenswürdige Prozesse nicht von der Untersuchung ausschließen / nicht ausschließen	Der Schalter aktiviert oder deaktiviert die Verwendung von konfigurierten Ausschlüsse nach Prozessen für die Komponente "Verhaltensanalyse". Der Schalter ist standardmäßig deaktiviert.
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Vollständiger Pfad des auszuschließenden Prozesses.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der App angewendet wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Sie können auch eine Liste von Ausnahmen aus einer Datei importieren, indem Sie auf die Schaltfläche **Importieren** klicken und die Liste der hinzugefügten Ausnahmen über die Schaltflächen **Exportieren** in eine Datei exportieren. Beim Importieren wird Ihnen vorgeschlagen, entweder die Liste der Ausnahmen zu ersetzen oder die Ausnahmen zu einer bestehenden Liste hinzuzufügen.

Fenster zum Hinzufügen des Ausschlussbereichs nach Prozessen

In diesem Fenster können Sie einen Ausschlussbereich nach Prozessen hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs

Einstellung	Beschreibung
Name des Ausschlussbereichs nach Prozess	Eingabefeld für den Namen des Ausschlussbereichs nach Prozessen. Dieser Name wird in der Tabelle im Fenster **Ausschlüsse nach Prozessen** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Ausschluss	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss dieses Bereichs

verwenden	während der Ausführung der App. Das Kontrollkästchen ist standardmäßig aktiviert.
Pfad des auszuschließenden Prozesses	Vollständiger Pfad des Prozesses, den Sie von der Untersuchung ausschließen möchten. Bei der Angabe des Pfades können Sie Masken verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Eingabefeld darf nicht leer sein.
Auf untergeordnete Prozesse anwenden	Untergeordnete Prozesse des Prozesses, der durch den Parameter **Pfad des auszuschließenden Prozesses** ausgeschlossen ist, ebenfalls von der Untersuchung ausschließen. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Verhaltensanalyse in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie Einstellungen zur Verhaltensanalyse für Apps in den Richtlinieneinstellungen konfigurieren (**Erweiterter Schutz** → **Verhaltensanalyse**).

Einstellungen der Komponente "Verhaltensanalyse"

Einstellung	Beschreibung
Verhaltensanalyse aktivieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Komponente "Verhaltensanalyse". Das Kontrollkästchen ist standardmäßig aktiviert.
Aktion, wenn schädliche Aktivitäten erkannt werden	Aktion, die Kaspersky Endpoint Security ausführen soll, wenn schädliche Aktivitäten im Betriebssystem erkannt werden: • App, die eine schädliche Aktivität ausführt **blockieren** (Standardwert). Kaspersky Endpoint Security beendet den Prozess, der schädliche Aktivität ausführt, und trägt Daten über die erkannte schädliche Aktivität in das Ereignisprotokoll ein. • **Informieren** Sie den Benutzer. Kaspersky Endpoint Security beendet den Prozess, der schädliche Aktivitäten ausführt, nicht, sondern protokolliert nur das Ereignis eines Funds schädliche Aktivität im Ereignisprotokoll.
Ausschluss nach	Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung von Ausschlüssen

Prozess	nach Prozess beim Betrieb der Komponente "Verhaltensanalyse". Dieses Kontrollkästchen ist standardmäßig deaktiviert. Durch Klicken auf die Schaltfläche **Konfigurieren** wird das Fenster **Ausschlüsse nach Prozess** geöffnet. In diesem Fenster können Sie den Ausschluss der Aktivität von Prozessen aus der Untersuchung konfigurieren.

Fenster "Ausschlüsse nach Prozess"

Die Tabelle enthält Ausschlussbereiche nach Prozessen. Mit dem Ausschlussbereich nach Prozessen können Sie einen Untersuchungsausschluss für die Aktivität des angegebenen Prozesses konfigurieren. Standardmäßig ist die Tabelle leer.

Wenn die Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response aktiviert ist, werden keine Ausschlüsse nach Prozess angewendet.

Einstellungen des Ausschlussbereichs nach Prozessen

Einstellung	Beschreibung
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Pfad	Vollständiger Pfad des auszuschließenden Prozesses.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der App angewendet wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Sie können auch eine Liste von Ausnahmen aus einer Datei importieren, indem Sie auf die Schaltfläche **Erweitert** -> **Importieren** klicken und die Liste der hinzugefügten Ausnahmen über die Schaltflächen **Erweitert** -> **Ausgewählte exportieren** oder **Erweitert** -> **Alle exportieren** in eine Datei exportieren. Beim Importieren wird Ihnen vorgeschlagen, entweder die Liste der Ausnahmen zu ersetzen oder die Ausnahmen zu einer bestehenden Liste hinzuzufügen.

Fenster "Vertrauenswürdiger Prozess"

In diesem Fenster können Sie einen Ausschlussbereich nach Prozessen hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs nach Prozessen

Einstellung	Beschreibung
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster **Ausschlüsse nach Prozessen** angezeigt.
Pfad des auszuschließenden	Vollständiger Pfad des Prozesses, den Sie von der Untersuchung ausschließen möchten. Bei der Angabe des Pfades können Sie Masken verwenden.

Prozesses	Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Eingabefeld darf nicht leer sein.
Auf untergeordnete Prozesse anwenden	Untergeordnete Prozesse des Prozesses, der durch den Parameter **Pfad des auszuschließenden Prozesses** ausgeschlossen ist, ebenfalls von der Untersuchung ausschließen. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert den Ausschluss dieses Bereichs von der Untersuchung während der Ausführung der App. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während ihrer Ausführung aus. Wenn das Kontrollkästchen deaktiviert ist, schließt die App diesen Bereich während ihrer Ausführung ein. Sie können diesen Bereich zu einem späteren Zeitpunkt ausschließen, indem Sie das Kontrollkästchen aktivieren. Das Kontrollkästchen ist standardmäßig aktiviert.

Verhaltensanalyse über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Analyse des Verhaltens von Apps im Betriebssystem mithilfe der vordefinierten Aufgabe "Verhaltensanalyse" (*Behavior_Detection*) verwalten.

Die Aufgabe "Verhaltensanalyse" wird standardmäßig ausgeführt. Sie können diese Aufgabe manuell starten und anhalten.

Sie können die Einstellungen für die Verhaltensanalyse konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zur Verhaltensanalyse ändern.

Einstellungen der Aufgabe zur Verhaltensanalyse

Einstellung	Beschreibung	Werte
`TaskMode`	Aktion, die von der App ausgeführt werden, wenn böswillige Aktivitäten im	`Block` (Standardwert) – Beendet den Prozess der App, die böswillige Aktivitäten ausführt.

	Betriebssystem erkannt werden.	`Notify` – Beendet den Prozess, der böswillige Aktivitäten ausführt, nicht, sondern protokolliert nur die Erkennung bösartiger Aktivitäten im Ereignisprotokoll.
`UseTrustedPrograms`	Prozesse von der Untersuchung ausschließen.	`Yes` – Aktivität der angegebenen Prozesse von der Untersuchung ausschließen. `No` (Standardwert) – Alle Prozesse untersuchen.
Der Abschnitt **[TrustedPrograms.item_#]** enthält Prozesse, die von der Untersuchung ausgeschlossen sind. Kaspersky Endpoint Security überwacht die Aktivität dieser Prozesse nicht.		
`ProgramPath`	Pfad des auszuschließenden Prozesses.	`<vollständiger Pfad des Prozesses>` – Prozess im angegebenen Verzeichnis von der Untersuchung ausschließen. Bei der Angabe des Pfades können Sie Masken verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.
`ApplyToDescendants`	Untergeordnete Prozesse des ausgeschlossenen Prozesses, der durch den `ProgramPath-` Parameter angegeben ist, von der Untersuchung ausschließen.	`Yes` – Schließt den angegebenen Prozess und alle seine untergeordneten Prozesse von der Untersuchung aus. `No` (Standardwert) – Nur den angegebenen Prozess von der Untersuchung ausschließen, untergeordnete Prozesse nicht von der Untersuchung ausschließen.
`ProgramDesc`	Beschreibung des ausgeschlossenen Prozesses.	
`UseTrustedProgram`	Ausschluss des angegebenen Prozesses von der	`Ja` (Standardwert) – Aktiviert für den angegebenen Prozess den Ausschluss der

	Untersuchung aktivieren.	Aktivität von der Untersuchung. `Nein` – Deaktiviert für den angegebenen Prozess den Ausschluss der Aktivität von der Untersuchung.

Verwendung von Kaspersky Security Network

Für einen effektiveren Schutz von Geräten und Benutzerdaten kann Kaspersky Endpoint Security das Kaspersky Security Network (KSN) verwenden. KSN ist eine cloudbasierte Wissensdatenbank von Kaspersky mit Reputationen zu Dateien, Internetressourcen und Software. Die Verwendung der Daten aus Kaspersky Security Network gewährleistet eine schnellere Reaktion auf verschiedene Bedrohungen, eine hohe Leistung der Schutzkomponenten und eine Verringerung der Anzahl von Fehlalarmen.

Die Verwendung von Kaspersky Security Network ist freiwillig. Sie können die Verwendung von KSN jederzeit aktivieren oder deaktivieren.

Diese Funktionalität wird im KESL-Container nicht unterstützt.

Infrastrukturlösungen von Kaspersky Security Network

Kaspersky Endpoint Security unterstützt die folgenden Infrastrukturlösungen für die Verwendung der Reputationsdatenbanken von Kaspersky:

- *Kaspersky Security Network (KSN)* – Eine Lösung, mit der Sie Informationen von Kaspersky erhalten. Gleichzeitig senden Sie Daten über Objekte, die auf Benutzergeräten gefunden wurden, zur zusätzlichen Überprüfung an Kaspersky, wo sie von Kaspersky-Analysten und geprüft werden und zur Ergänzung in die Reputations- und Statistikdatenbanken eingehen.

- *Kaspersky Private Security Network (KPSN)* ist eine Lösung, die es Benutzern von Geräten mit installiertem Kaspersky Endpoint Security ermöglicht, auf die Reputationsdatenbanken und weitere statistische Daten von Kaspersky zuzugreifen, ohne dabei Daten von ihren Geräten an Kaspersky zu senden. KPSN ist für Unternehmenskunden konzipiert, die Kaspersky Security Network beispielsweise aus folgenden Gründen nicht nutzen können:

  - Lokale Arbeitsplätze haben keine Verbindung mit dem Internet.

  - Es gelten gesetzliche oder unternehmensinterne sicherheitsbezogene Einschränkungen, die es verbieten, Daten über die Grenzen des Landes oder des lokalen Netzwerks der Organisation hinaus zu senden.

Nachdem Sie die App unter einer neuen Lizenz zur Nutzung von KPSN aktiviert haben, müssen Sie Ihrem Provider die Informationen über den neuen Lizenzschlüssel zur Verfügung stellen. Andernfalls ist der Austausch von Informationen mit KPSN aufgrund eines Authentifizierungsfehlers unmöglich.

Möglichkeiten zur Verwendung von Kaspersky Security Network

Es gibt zwei Möglichkeiten, KSN zu verwenden:

- **Erweiterter KSN-Modus** – Erlaubt Ihnen das Abrufen von Informationen aus der Wissensdatenbank von Kaspersky, während Kaspersky Endpoint Security automatisch statistische Informationen an Kaspersky Security Network sendet, die im Rahmen seiner Ausführung entstehen. Ferner kann die App Dateien (oder Teile von Dateien), die von Angreifern zur Beschädigung des Geräts oder der Daten verwendet werden können, zur erweiterten Untersuchung an Kaspersky senden.

- **Standardmäßiger KSN-Modus** – Erlaubt Ihnen das Abrufen von Informationen aus der Wissensdatenbank von Kaspersky, während Kaspersky Endpoint Security keine anonymen Statistiken und Daten über Arten und Quellen von Bedrohungen sendet.

Sie können jederzeit eine zwischen den Optionen für die Nutzung von Kaspersky Security Network wechseln.

Es werden keinerlei persönliche Daten des Benutzers erfasst, verarbeitet und gespeichert. Detaillierte Informationen über den Versand, die Speicherung und Vernichtung von während der Ausführung von KSN erfassten statistischen Informationen finden Sie in der Erklärung zu Kaspersky Security Network und auf der Website von Kaspersky. Die Datei mit dem Text der Erklärung zu Kaspersky Security Network ist im Lieferumfang der App enthalten.

Cloud-Modus von Kaspersky Endpoint Security

Der *Cloud-Modus* ist ein Modus zur Ausführung von Kaspersky Endpoint Security, in dem die App eine schlankere Version der Malware-Datenbanken verwendet. Dies reduziert die Belastung des Arbeitsspeichers des Geräts.

Die App-Ausführung mit den schlanken Malware-Datenbanken erfolgt über Kaspersky Security Network.

Wenn Kaspersky Endpoint Security im Standard-Modus verwendet wird und Sie im Rahmen der App-Ausführung KSN verwenden, können Sie den Cloud-Modus der App aktivieren.

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, wird die Verwendung der schlankeren Malware-Datenbanken nicht unterstützt. Die App erhält vom Schutzserver spezielle Datenbanken, die für den Betrieb des Light Agent erforderlich sind.

Kaspersky Endpoint Security wechselt zur Verwendung der schlankeren Version der Malware-Datenbanken, nachdem der Cloud-Modus aktiviert wurde und das nächste Update der Datenbanken und App-Module durchgeführt wurde. Wenn der Cloud-Modus deaktiviert wird, lädt Kaspersky Endpoint Security beim nächsten Update die vollständige Version der App-Datenbanken von den Kaspersky-Servern herunter und aktualisiert die Datenbanken und Module der App.

Wenn Sie KSN nicht verwenden oder der Cloud-Modus deaktiviert ist, verwendet Kaspersky Endpoint Security die Vollversion der Programmdatenbanken.

Der Cloud-Modus wird automatisch deaktiviert, wenn KSN deaktiviert ist.

Verwendung des Dienstes für den KSN-Proxy-Server

Benutzergeräte, die unter Verwaltung des Administrationsservers stehen, können entweder direkt oder über den KSN Proxy-Service mit KSN interagieren.

Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, wird die Interaktion mit der KSN-Infrastruktur über den KSN Proxy-Service realisiert. Die direkte Interaktion mit KSN wird nicht unterstützt. Wenn der KSN-Proxy-Server nicht verfügbar ist, wird zur Ausführung der App kein KSN verwendet.

Der Proxy-Server von KSN bietet die folgenden Funktionen:

- Benutzergeräte können selbst dann Anfragen und Informationen an KSN senden, wenn sie über keinen direkten Internetzugriff verfügen.
- Die verarbeiteten Daten werden vom Proxy-Server von KSN im Cache zwischengespeichert, wodurch die Belastung für den ausgehenden Datenverkehr verringert und das Empfangen der abgefragten Informationen

durch das Benutzergerät beschleunigt wird.

Sie können die Einstellungen des KSN Proxy-Server in den Eigenschaften des Administrationsservers konfigurieren. Weitere Informationen zum Proxy-Server von KSN finden Sie in der Hilfe von Kaspersky Security Center.

Verwendung von Kaspersky Security Network in der Web Console konfigurieren

In der Web Console können Sie die Verwendung von Kaspersky Security Network bei der Ausführung von Kaspersky Endpoint Security in der Richtlinie konfigurieren (**Programmeinstellungen** → **Erweiterter Schutz** → **Kaspersky Security Network**).

Den Text der Erklärung zu Kaspersky Security Network können Sie im Fenster **Erklärung zu Kaspersky Security Network** lesen, welches Sie über den Link **Erklärung zu Kaspersky Security Network** öffnen können.

Informationen zur Verfügbarkeit von KSN werden in Kaspersky Security Center anhand des Status des Client-Geräts (*OK, Kritisch, Warnung*) in der Liste der verwalteten Geräte auf der Registerkarte **Assets (Geräte)** angezeigt.

Parameter zur Verwendung von Kaspersky Security Network

Einstellung	Beschreibung
KSN nicht verwenden	Wenn Sie diese Option auswählen, lehnen Sie die Verwendung von Kaspersky Security Network ab.
Erweiterter KSN-Modus	Wenn Sie diese Option auswählen, akzeptieren Sie die Bedingungen zur Verwendung von Kaspersky Security Network. Sie erhalten Informationen aus der Online-Wissensdatenbank von Kaspersky über die Reputation von Dateien, Webressourcen und Software. Es werden zudem anonymisierte Statistikdaten und Informationen zu Typen und Quellen von verschiedenen Bedrohungen an Kaspersky gesendet, um Kaspersky Security Network zu verbessern.
Standardmäßiger KSN-Modus	Wenn Sie diese Option auswählen, akzeptieren Sie die Bedingungen zur Verwendung von Kaspersky Security Network. Sie erhalten Informationen aus der Online-Wissensdatenbank von Kaspersky über die Reputation von Dateien, Webressourcen und Software.
Cloud-Modus aktivieren	Das Kontrollkästchen aktiviert oder deaktiviert den Ausführungsmodus, in dem Kaspersky Endpoint Security eine schlankere Version der Malware-Datenbanken verwendet. Das Kontrollkästchen ist verfügbar, wenn KSN aktiviert ist. Das Kontrollkästchen ist aktiviert, wenn Sie beim Erstellen der Richtlinie die Bedingungen der Erklärung zu Kaspersky Security Network akzeptiert haben und den erweiterten KSN-Modus verwenden. Der Modus wird nach dem nächsten Update der App-Datenbanken aktiviert oder deaktiviert. Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.
KSN-Server verwenden, wenn KSN-Proxy-	Das Kontrollkästchen aktiviert oder deaktiviert die Möglichkeit, direkt mit KSN-Servern zu kommunizieren, wenn der KSN Proxy-Server nicht verfügbar ist. Das Kontrollkästchen ist standardmäßig aktiviert.

Server nicht verfügbar	Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.
Erklärung zu Kaspersky Security Network	Der Link öffnet das Fenster **Erklärung zu Kaspersky Security Network**, in dem Sie den Text der Erklärung zu Kaspersky Security Network lesen können.

Erklärung zu Kaspersky Security Network

In diesem Fenster können Sie den Text der Erklärung zu Kaspersky Security Network lesen und die Bedingungen akzeptieren.

Einstellungen für Kaspersky Security Network

Einstellung	Beschreibung
Ich bestätige, dass ich die Bestimmungen und Bedingungen der Erklärung zu Kaspersky Security Network vollständig gelesen habe, und sie verstehe und akzeptiere.	Wenn Sie diese Option auswählen, bestätigen Sie, dass Sie Kaspersky Security Network verwenden möchten und dass Sie die Bedingungen der angezeigten Erklärung zu Kaspersky Security Network vollständig gelesen haben, und sie verstehen und akzeptieren.
Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Security Network nicht.	Wenn Sie diese Option auswählen, bestätigen Sie, dass Sie Kaspersky Security Network nicht verwenden möchten.

Verwendung von Kaspersky Security Network in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Verwendung von Kaspersky Security Network bei der Ausführung von Kaspersky Endpoint Security in den Richtlinieneinstellungen konfigurieren (**Erweiterter Schutz** → **Kaspersky Security Network**).

Den Text der Erklärung zu Kaspersky Security Network können Sie im Fenster **Erklärung zu Kaspersky Security Network** lesen, welches Sie über den Link **Erklärung zu Kaspersky Security Network** öffnen können.

Informationen zur Verfügbarkeit von KSN werden in Kaspersky Security Center anhand des Status des Client-Geräts (*OK, Kritisch, Warnung*) in der Liste der verwalteten Geräte auf der Registerkarte **Geräte** angezeigt.

Parameter zur Verwendung von Kaspersky Security Network

Einstellung	Beschreibung
Erklärung zu Kaspersky Security Network	Dieser Link öffnet das Fenster **Erklärung zu Kaspersky Security Network**. In diesem Fenster können Sie den Text der Erklärung zu Kaspersky Security Network einsehen.
Kaspersky Security Network (KSN)	In diesem Block werden Informationen darüber angezeigt, welche Option der KSN-Nutzung aktiviert ist und ob KSN zur Ausführung von Kaspersky Endpoint Security verwendet wird oder nicht. Durch Klicken auf die Schaltfläche **Ändern** öffnet sich ein Fenster, in dem Sie die Verwendung des Kaspersky Security Network konfigurieren können.

Cloud-Modus aktivieren	Das Kontrollkästchen aktiviert oder deaktiviert den Ausführungsmodus, in dem Kaspersky Endpoint Security eine schlankere Version der Malware-Datenbanken verwendet. Das Kontrollkästchen ist verfügbar, wenn KSN aktiviert ist. Das Kontrollkästchen ist aktiviert, wenn Sie beim Erstellen der Richtlinie die Bedingungen der Erklärung zu Kaspersky Security Network akzeptiert haben und den erweiterten KSN-Modus verwenden. Der Modus wird nach dem nächsten Update der App-Datenbanken aktiviert oder deaktiviert. Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.
KSN-Server verwenden, wenn KSN-Proxy-Server nicht verfügbar	Das Kontrollkästchen aktiviert oder deaktiviert die Möglichkeit, direkt mit KSN-Servern zu kommunizieren, wenn der KSN Proxy-Server nicht verfügbar ist. Das Kontrollkästchen ist standardmäßig aktiviert. Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.

Einstellungen für Kaspersky Security Network

In diesem Fenster können Sie die Einstellungen zur Verwendung von Kaspersky Security Network anpassen.

Einstellungen für Kaspersky Security Network

Einstellung	Beschreibung
Weitere Informationen...	Dieser Link öffnet die Website von Kaspersky.
Kaspersky Security Network nicht verwenden	Wenn Sie diese Option auswählen, lehnen Sie die Verwendung von Kaspersky Security Network ab.
Standardmäßiger KSN-Modus	Wenn Sie diese Option auswählen, akzeptieren Sie die Bedingungen zur Verwendung von Kaspersky Security Network. Sie erhalten Informationen aus der Wissensdatenbank von Kaspersky über die Reputation von Dateien, Webressourcen und Software.
Erweiterter KSN-Modus	Wenn Sie diese Option auswählen, akzeptieren Sie die Bedingungen zur Verwendung von Kaspersky Security Network. Sie erhalten Informationen aus der Wissensdatenbank von Kaspersky über die Reputation von Dateien, Webressourcen und Software. Es werden zudem anonymisierte Statistikdaten und Informationen zu Typen und Quellen von verschiedenen Bedrohungen an Kaspersky gesendet, um Kaspersky Security Network zu verbessern.
Erklärung zu Kaspersky Security Network	Der Link öffnet das Fenster **Erklärung zu Kaspersky Security Network, in dem** Sie den Text der Erklärung zu Kaspersky Security Network lesen können.

Erklärung zu Kaspersky Security Network

In diesem Fenster können Sie den Text der Erklärung zu Kaspersky Security Network lesen und die Bedingungen akzeptieren.

Einstellungen für Kaspersky Security Network

Einstellung	Beschreibung
Ich bestätige, dass ich die Bestimmungen und Bedingungen der Erklärung zu Kaspersky Security Network vollständig gelesen habe, und sie verstehe und akzeptiere.	Wenn Sie diese Option auswählen, bestätigen Sie, dass Sie Kaspersky Security Network verwenden möchten und dass Sie die Bedingungen der angezeigten Erklärung zu Kaspersky Security Network vollständig gelesen haben, und sie verstehen und akzeptieren. Die Option ist verfügbar, wenn Sie im Fenster **Einstellungen von Kaspersky Security Network** die Option **Standardmäßiger KSN-Modus** oder **Erweiterter KSN-Modus** ausgewählt haben.
Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Security Network nicht.	Wenn Sie diese Option auswählen, bestätigen Sie, dass Sie Kaspersky Security Network nicht verwenden möchten. Die Option ist verfügbar, wenn Sie im Fenster **Einstellungen von Kaspersky Security Network** die Option **Standard KSN-Modus** oder **Erweiterter KSN-Modus** ausgewählt haben.

Verwendung von Kaspersky Security Network über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Verwendung von Kaspersky Security Network mithilfe des Parameters `UseKSN` in den allgemeinen App-Einstellungen aktivieren und deaktivieren.

Sie können den Wert des Parameters `UseKSN` mithilfe von Befehlszeilenschaltern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen App-Einstellungen enthält.

Um die Verwendung von Kaspersky Security Network mithilfe von Befehlszeilenschaltern zu aktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings UseKSN=<Extended/Basic> --accept-ksn
```

Wobei gilt:

- `<Extended/Basic>` – Modus zur Verwendung von Kaspersky Security Network.
- `--accept-ksn` – Schalter, der bedeutet, dass Sie den in der Erklärung zu Kaspersky Security Network dargelegten Bedingungen zustimmen. Ich bestätige, dass ich die Bedingungen der Erklärung zu Kaspersky Security Network vollständig gelesen habe und sie verstehe und akzeptiere.

Die Datei "ksn_licence.<ID der Sprache>", die den Text der Erklärung zu Kaspersky Security Network enthält, befindet sich im Verzeichnis opt/kaspersky/kesl/doc/.

Um die Verwendung von Kaspersky Security Network mithilfe von Befehlszeilenschaltern zu deaktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings UseKSN=No
```

Um die Nutzung von Kaspersky Security Network mithilfe einer Konfigurationsdatei zu aktivieren oder zu deaktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings --file <Name der Konfigurationsdatei> [--json] [--accept-ksn]
```

Wobei gilt:

- `--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei mit den allgemeinen App-Einstellungen, in der der gewünschte Wert des Parameters `UseKSN` konfiguriert ist.
- `--json` – Geben Sie diesen Schalter an, wenn Sie Einstellungen aus einer Konfigurationsdatei im JSON-Format importieren. Wenn Sie den Schalter `--json` nicht angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.
- `--accept-ksn` – Schalter, der bedeutet, dass Sie den in der Erklärung zu Kaspersky Security Network dargelegten Bedingungen zustimmen. Der Schalter ist erforderlich, wenn Sie die Verwendung von Kaspersky Security Network aktivieren.

Wenn die App Kaspersky Endpoint Security auf einem Client-Gerät installiert ist und unter einer Richtlinie arbeitet, die in Kaspersky Security Center zugewiesen wurde, kann der Wert der Einstellung `UseKSN` nur mithilfe von Kaspersky Security Center geändert werden. Wenn die App Kaspersky Endpoint Security auf einem Client-Gerät installiert ist und nicht mehr von der Richtlinie verwaltet wird, wird als Wert der Einstellung `UseKSN=No` festgelegt.

Verbindung mit Kaspersky Security Network über die Befehlszeile prüfen

Um die Verbindung mit Kaspersky Security Network zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --app-info
```

Die Zeile **Verwendung von Kaspersky Security Network** zeigt den Status der Verbindung mit Kaspersky Security Network an:

- Wenn als Status `Erweiterter KSN-Modus` angezeigt wird, ist Kaspersky Endpoint Security mit Kaspersky Security Network verbunden: Es können Informationen aus der Wissensdatenbank abgerufen werden und anonyme Statistikdaten und Informationen über die Typen und Quellen der Bedrohungen gesendet werden.
- Wenn als Status `Standardmäßiger KSN-Modus` angezeigt wird, ist Kaspersky Endpoint Security mit Kaspersky Security Network verbunden: Es können Informationen aus der Wissensdatenbank abgerufen werden, aber es werden keine anonymen Statistikdaten und Informationen über die Typen und Quellen der Bedrohungen gesendet.
- Wenn der Status `Nicht aktiviert` angezeigt wird, ist Kaspersky Endpoint Security nicht mit Kaspersky Security Network verbunden.

In der Zeile **Infrastrukturlösung von Kaspersky Security Network**, werden die Informationen zu der Infrastrukturlösung angezeigt, die für die Interaktion mit den Reputationsdatenbanken von Kaspersky verwendet wird: `Kaspersky Security Network` oder `Kaspersky Private Security Network`.

Mögliche Gründe, warum keine Verbindung mit Kaspersky Security Network besteht:

- Das Gerät des Benutzers ist nicht mit dem Internet verbunden.
- Die Verwendung von Kaspersky Security Network ist nicht aktiviert.
- Die App wurde nicht aktiviert oder die Lizenz ist abgelaufen.
- Es wurden Probleme im Zusammenhang mit dem Lizenzschlüssel gefunden. Beispielsweise könnte der Schlüssel auf der Deny-Liste stehen.

Cloud-Modus über die Befehlszeile aktivieren oder deaktivieren

Der *Cloud-Modus* ist ein Modus zur Ausführung von Kaspersky Endpoint Security, in dem die App eine schlankere Version der Malware-Datenbanken verwendet.

> Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, wird die Verwendung der schlankeren Malware-Datenbanken nicht unterstützt. Die App erhält vom Schutzserver spezielle Datenbanken, die für den Betrieb des Light Agent erforderlich sind.

Über die Befehlszeile können Sie den Cloud-Modus mithilfe des Parameters `CloudMode=Yes/No` in den allgemeinen App-Einstellungen aktivieren oder deaktivieren.

Sie können den Wert des Parameters `CloudMode` mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen App-Einstellungen enthält, oder mithilfe von Befehlszeilenschaltern.

> Der Cloud-Modus der App ist bei aktivierter Verwendung von Kaspersky Security Network verfügbar.

Erweiterte Einstellungen für die Ausführung der App

Sie können die folgenden zusätzlichen Einstellungen für die Ausführung der App konfigurieren:

- Verwendung eines Proxy-Servers im Rahmen der App-Ausführung.
- Globale Ausschlüsse zum Ausschließen von Mountpunkten aus dem Modul zum Abfangen für Dateioperationen der Komponenten zum Schutz vor bedrohlichen Dateien, zum Schutz vor Verschlüsselung und zur Container-Überwachung, sowie der Aufgaben zur Schadsoftware-Untersuchung, zur Untersuchung wichtiger Bereiche, zur Untersuchung von Containern und zur Untersuchung von Wechseldatenträgern.
- Prozess-Speicher von der Untersuchung ausschließen.
- Modus des Modul zum Abfangen von Dateioperationen.
- Erkennung legitimer Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können.
- Überwachung der Anwendungsstabilität.
- Starteinstellungen der Anwendung.
- Begrenzung der Nutzung von Speicher- und CPU-Ressourcen für Untersuchungsaufgaben.
- Begrenzung des von der App verwendeten residenten Speichers.
- Begrenzung der Anzahl benutzerdefinierter Untersuchungsaufgaben, die ein nicht privilegierter Benutzer gleichzeitig ausführen kann.
- Einstellungen zur Übertragung von Informationen an den Kaspersky Security Center.
- Berechtigungen für die Verwaltung von Aufgaben.

Proxy-Server konfigurieren

Sie können die Proxy-Server-Einstellungen konfigurieren, wenn Benutzer von Client-Geräten über einen Proxy-Server auf das Internet zugreifen. Kaspersky Endpoint Security kann einen Proxy-Server verwenden, um sich mit den Kaspersky-Servern zu verbinden, um beispielsweise die Datenbanken und Module zu aktualisieren oder um mit Kaspersky Security Network und Kaspersky Endpoint Detection and Response (KATA) zu kommunizieren.

Standardmäßig ist die Verwendung eines Proxy-Servers deaktiviert.

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, wird die Verwendung eines Proxy-Servers für die Verbindung mit Kaspersky Security Network, zur SVM und zum Integrationsserver nicht unterstützt.

Proxy-Server-Einstellungen in der Web Console konfigurieren

In der Web Console können Sie die Verwendung eines Proxy-Servers in den Richtlinieneinstellungen konfigurieren (**App-Einstellungen** → **Allgemeine Einstellungen** → **Proxy-Server-Einstellungen**).

Proxy-Server-Einstellungen

Einstellung	Beschreibung
Keinen Proxy-Server verwenden	Wenn diese Option ausgewählt ist, wird der Proxy-Server bei der Ausführung der App nicht verwendet.
Angegebene Proxy-Server-Einstellungen verwenden	Wenn diese Option ausgewählt ist, verwendet die App die angegebenen Einstellungen des Proxy-Servers, beispielsweise für die Integration mit Kaspersky Endpoint Detection and Response (KATA).
Adresse	Eingabefeld für die IP-Adresse oder den Domänennamen des Proxy-Servers. Dieses Feld ist verfügbar, wenn die Option **Angegebene Einstellungen des Proxy-Servers verwenden** ausgewählt ist.
Port	Eingabefeld für den Port des Proxy-Servers. Standardwert: 3128. Dieses Feld ist verfügbar, wenn die Option **Angegebene Einstellungen des Proxy-Servers verwenden** ausgewählt ist.
Authentifizierung am Proxy-Server verwenden	Aktiviert oder deaktiviert die Authentifizierung mithilfe von Benutzername und Kennwort beim Zugriff auf den Proxy-Server. Das Kontrollkästchen ist verfügbar, wenn die Variante **Angegebene Einstellungen des Proxy-Servers verwenden** ausgewählt ist. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Für die Verbindung über einen Proxy-Server mittels HTTP-Protokoll wird empfohlen, ein separates Konto zu verwenden, das nicht zur Authentifizierung in anderen Systemen verwendet wird. Der HTTP-Proxy-Server verwendet eine unsichere Verbindung und dessen Konto kann kompromittiert werden.
Benutzername	Eingabefeld für den Benutzernamen zur Authentifizierung des Benutzers auf dem Proxy-Server. Das Eingabefeld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxy-Server verwenden** aktiviert ist.
Bearbeiten	Ermöglicht die Angabe eines Benutzerkennworts für die Autorisierung auf dem Proxy-Server. Das Feld **Kennwort** kann nicht bearbeitet werden. Standardmäßig ist das Kennwort leer. Um ein Kennwort anzugeben, klicken Sie auf die Schaltfläche **Bearbeiten**, geben Sie im sich öffnenden Fenster das Kennwort ein und klicken Sie auf die Schaltfläche **OK**. Es wird empfohlen, sicherzustellen, dass die Passwortkomplexität und die Anti-Brute-Force-Mechanismen gewährleisten, dass das Passwort innerhalb von 6 Monaten nicht geknackt werden kann. Wenn Sie im Fenster zur Kennworteingabe auf die Schaltfläche **Anzeigen** klicken, wird das Kennwort im Klartext angezeigt. Die Schaltfläche ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxy-Server verwenden** aktiviert ist.

Kaspersky Security Center als Proxy-Server für die Aktivierung der App verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Verwendung von Kaspersky Security Center als Proxy-Server für die Aktivierung der App. Wenn dieses Kontrollkästchen aktiviert ist, wird Kaspersky Security Center von Kaspersky Endpoint Security als Proxy-Server zur Aktivierung der App verwendet. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird. Wenn die App im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, stellt der Schutzserver die Lizenzinformationen bereit.

Proxy-Server-Einstellungen in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Verwendung eines Proxy-Servers in den Richtlinieneinstellungen konfigurieren (**Allgemeine Einstellungen** → **Proxy-Server-Einstellungen**).

Proxy-Server-Einstellungen

Einstellung	Beschreibung
Keinen Proxy-Server verwenden	Wenn diese Option ausgewählt ist, wird der Proxy-Server bei der Ausführung der App nicht verwendet.
Angegebene Proxy-Server-Einstellungen verwenden	Wenn diese Option ausgewählt ist, verwendet die App die angegebenen Einstellungen des Proxy-Servers, beispielsweise für die Integration mit Kaspersky Endpoint Detection and Response (KATA).
Adresse und Port	Felder zur Eingabe der IP-Adresse bzw. des Domänennamens und des Ports des Proxy-Servers. Standardwert: 3128. Die Felder sind verfügbar, wenn die Option **Angegebene Einstellungen des Proxy-Servers verwenden** ausgewählt ist.
Authentifizierung am Proxy-Server verwenden	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Authentifizierung mithilfe von Benutzername und Kennwort beim Zugriff auf den Proxy-Server. Das Kontrollkästchen ist verfügbar, wenn die Variante **Angegebene Einstellungen des Proxy-Servers verwenden** ausgewählt ist. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Für die Verbindung über einen Proxy-Server mittels HTTP-Protokoll wird empfohlen, ein separates Konto zu verwenden, das nicht zur Authentifizierung in anderen Systemen verwendet wird. Der HTTP-Proxy-Server verwendet eine unsichere Verbindung und dessen Konto kann kompromittiert werden.
Benutzername	Eingabefeld für den Benutzernamen zur Authentifizierung des Benutzers auf dem Proxy-Server. Das Eingabefeld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxy-Server verwenden** aktiviert ist.
Kennwort	Eingabefeld für das Kennwort des Benutzers zur Authentifizierung auf dem Proxy-

	Server. Es wird empfohlen, sicherzustellen, dass die Passwortkomplexität und die Anti-Brute-Force-Mechanismen gewährleisten, dass das Passwort innerhalb von 6 Monaten nicht geknackt werden kann. Ein Klick auf die Schaltfläche **Anzeigen** zeigt das Kennwort des Benutzers im Feld **Kennwort** in unverschlüsselter Form an. Standardmäßig wird das Kennwort des Benutzers verschlüsselt und wird in Form von Punkten angezeigt. Das Eingabefeld und die Schaltfläche sind verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxy-Server verwenden** aktiviert ist.
Kaspersky Security Center als Proxy-Server für die Aktivierung der App verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Verwendung von Kaspersky Security Center als Proxy-Server für die Aktivierung der App. Wenn dieses Kontrollkästchen aktiviert ist, wird Kaspersky Security Center von Kaspersky Endpoint Security als Proxy-Server zur Aktivierung der App verwendet. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird. Wenn die App im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, stellt der Schutzserver die Lizenzinformationen bereit.

Proxy-Server-Einstellungen über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Verwendung eines Proxy-Servers durch die Komponenten der App aktivieren und deaktivieren, indem Sie die Parameter `UseProxy` und `Proxy-Server` in den allgemeinen App-Einstellungen verwenden.

Sie können den Wert von Parametern mithilfe von Befehlszeilenschaltern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen App-Einstellungen enthält.

Der Parameter `UseProxy` kann die folgenden Werte annehmen:

- `Yes` – Nutzung eines Proxy-Servers aktivieren.
- `No` – Nutzung eines Proxy-Servers deaktivieren.

Mit dem Parameter `ProxyServer` können Sie Proxy-Server-Parameter im Format `[<Benutzer>[:<Kennwort>]@]<Proxy-Server-Adresse>[:<Port>]` angeben, wobei gilt:

- `<Benutzer>` – Benutzername für die Authentifizierung auf dem Proxy-Server.
- `<Kennwort>` – Benutzerkennworts für die Autorisierung auf dem Proxy-Server.
- `<Proxy-Server-Adresse>` – IP-Adresse oder Domänenname des Proxy-Servers.
- `<Port>` – Port des Proxy-Servers.

Wenn für die Verbindung mit einem Proxy-Server keine Authentifizierung erforderlich ist, müssen Sie den Parameter `ProxyServer` nicht angeben.

Für die Verbindung über einen Proxy-Server mittels HTTP-Protokoll wird empfohlen, ein separates Konto zu verwenden, das nicht zur Authentifizierung in anderen Systemen verwendet wird. Der HTTP-Proxy-Server verwendet eine unsichere Verbindung und dessen Konto kann kompromittiert werden.

Globale Ausschlüsse konfigurieren

Sie können globale Ausschlüsse konfigurieren, um Mountpunkte aus dem Modul zum Abfangen für Dateioperationen der folgenden Komponenten und Untersuchungsaufgaben auszuschließen: Komponenten zum Schutz vor bedrohlichen Dateien und zum Schutz vor Verschlüsselung, sowie Aufgaben zur Schadsoftware-Untersuchung, zur Untersuchung wichtiger Bereiche und zur Untersuchung von Containern. Durch das Ausschließen von Mountpunkten können Sie lokale oder Remote-Verzeichnisse, die auf dem Gerät gemountet sind, vom Modul zum Abfangen von Dateioperationen ausschließen. Darüber hinaus wirken sich globale Ausnahmen auf die Ausführung der Komponente Container-Überwachung“ und der Aufgabe Untersuchung von Wechseldatenträgern aus.

Globale Ausschlüsse in der Web Console konfigurieren

In der Web Console können Sie globale Ausschlüsse in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen → Allgemeine Einstellungen → Globale Ausschlüsse**).

Die Tabelle im Abschnitt **Globale Ausnahmen** enthält Mountpunkte, die vom Modul zum Abfangen von Dateioperationen ausgeschlossen werden.

In der Spalte **Pfad** werden Pfade der ausgeschlossene Mountpunkte angezeigt. Standardmäßig die Tabelle leer.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Fenster zum Hinzufügen eines ausgeschlossenen Mountpunkts

Einstellungen des Mountpunkts

Einstellung	Beschreibung
Dateisystem, Zugriffsprotokoll und Pfad	In der Dropdown-Liste können Sie den Typ des Dateisystems auswählen, auf dem sich die Verzeichnisse befinden, die Sie zu den Ausschlüssen von der Untersuchung hinzufügen möchten: • **Lokal** – Lokale Mountpunkte. • **Mounted** – Remote-Verzeichnisse, die auf dem Gerät über das Samba- oder NFS-Protokoll eingebunden sind.

	• **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind.
Zugriffsprotokoll	In der Dropdown-Liste können Sie das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind. Diese Dropdown-Liste ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** ausgewählt ist.
Pfad	Eingabefeld für den Pfad des Mountpunkts, den Sie zu den Ausschlüssen des Moduls zum Abfangen von Dateioperationen hinzufügen möchten. Bei der Angabe des Pfades können Sie Masken verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Lokal** ausgewählt ist.
Name der freigegebenen Ressource	Eingabefeld für den Namen der freigegebenen Ressource des Dateisystems, auf der sich die Verzeichnisse befinden, die Sie zu den Ausschlüssen des Moduls zum Abfangen von Dateioperationen hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste **Zugriffsprotokoll** das Element **Benutzerdefiniert** ausgewählt sind.

Globale Ausschlüsse in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie globale Ausschlüsse in den Richtlinieneigenschaften konfigurieren (**Allgemeine Einstellungen** → **Globale Ausschlüsse**).

Die Einstellungsgruppe **Ausgeschlossene Mountpunkte** enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausgeschlossene Mountpunkte** öffnet.

Die Liste im Fenster enthält die Pfade der ausgeschlossene Mountpunkte. Standardmäßig ist die Liste leer.

Sie können Elemente in der Liste hinzufügen, bearbeiten und löschen.

Ein Klick auf die Schaltfläche **Löschen** entfernt das ausgewählte Element aus der Tabelle.

Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.

Fenster "Pfad zum Mountpunkt"

Einstellungen des Mountpunkts

Einstellung	Beschreibung
Dateisystem, Zugriffsprotokoll und Pfad	In dieser Einstellungsgruppe können Sie die Position des Mountpunkts angeben. In der Dropdown-Liste der Dateisysteme können Sie den Typ des Dateisystems auswählen, auf dem sich die Verzeichnisse befinden, die Sie zu den Ausschlüssen von der Untersuchung hinzufügen möchten: • **Lokal** – Lokale Mountpunkte. • **Mounted** – Remote-Verzeichnisse, die auf dem Gerät über das Samba- oder NFS-Protokoll eingebunden sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind.
	Wenn in der Drop-down-Liste der Dateisysteme der Typ **Mounted** ausgewählt ist, können Sie rechts in der Drop-down-Liste das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Alle Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind.
	Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu dem Mountpunkt angeben, den Sie zu den Ausschlüssen des

	Moduls zum Abfangen von Dateioperationen hinzufügen möchten. Bei der Angabe des Pfades können Sie Masken verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.
Name des Dateisystems	Eingabefeld für den Namen des Dateisystems, auf dem sich die Verzeichnisse befinden, die Sie zu den Ausschlüssen des Moduls zum Abfangen von Dateioperationen hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste auf der rechten Seite das Element **Benutzerdefiniert** ausgewählt sind.

Globale Ausschlüsse über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie den Ausschluss von Mountpunkten mithilfe des Parameters `ExcludedMountPoint.item_#` in den allgemeinen App-Einstellungen konfigurieren.

Sie können den Wert des Parameters mithilfe von Befehlszeilenschaltern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen App-Einstellungen enthält.

Der Parameter `ExcludedMountPoint.item_#` kann die folgenden Werte annehmen:

- `AllRemoteMounted` – Alle Remote-Verzeichnisse, die auf dem Gerät über SMB- oder NFS-Protokolle gemountet sind, werden vom Modul zum Abfangen von Dateioperationen ausgeschlossen.
- `Mounted:NFS` – Alle Remote-Verzeichnisse, die auf dem Gerät über NFS-Protokolle gemountet sind, werden vom Modul zum Abfangen von Dateioperationen ausgeschlossen.

- `Mounted:SMB` – Alle Remote-Verzeichnisse, die auf dem Gerät über SMB-Protokolle gemountet sind, werden vom Modul zum Abfangen von Dateioperationen ausgeschlossen.
- `Mounted:<Typ des Dateisystems>` – alle eingebundenen Verzeichnisse mit dem angegebenen Dateisystem werden vom Modul zum Abfangen von Dateioperationen ausgeschlossen.
- `/mnt` – Objekte im Mountpunkt /mnt (einschließlich Unterverzeichnissen), welcher als temporärer Mountpunkt für Wechseldatenträger dient, werden vom Abfangen ausgeschlossen.
- `<Pfad mit der Maske /mnt/user* oder /mnt/**/user_share>` – Objekte im Mountpunkt, deren Namen der angegebenen Maske entsprechen, werden vom Abfangen ausgeschlossen.

  Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

  Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

  Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

  Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

  Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben.

  Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst.

  Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Sie können mehrere Mountpunkte angeben, die Sie von der Untersuchung ausschließen möchten.

Die Mountpunkte müssen genau so angegeben werden, wie sie in der Ausgabe des Befehls `mount` angezeigt werden.

Prozess-Speicher von der Untersuchung ausschließen

Sie können Untersuchungsausschlüsse für den Prozess-Speicher konfigurieren. Der Arbeitsspeicher der angegebenen Prozesse wird von der App nicht untersucht.

Ausschlüsse in der Web Console konfigurieren

In der Web Console können Sie Untersuchungsausschlüsse für den Prozess-Speicher in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen** → **Allgemeine Einstellungen** → **App-Einstellungen**).

Durch Klicken auf den Link **Ausschluss des Prozess-Speichers von der Untersuchung konfigurieren** im Block **Prozess-Speicher von Untersuchung ausschließen** wird das Fenster **Prozess-Speicher von Untersuchung ausschließen** geöffnet, in dem Sie eine Liste mit Ausschlüssen erstellen können.

Die Liste im Fenster **Prozess-Speicher von der Untersuchung ausschließen** enthält Pfade zu Prozessen, die die App von der Untersuchung des Prozess-Speichers ausschließt. Bei der Angabe des Pfades können Sie Masken verwenden. Standardmäßig ist die Liste leer.

Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben.

Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst.

Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Sie können Elemente in der Liste hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security den ausgewählten Prozesspfad aus der Liste.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens ein Prozesspfad ausgewählt ist.

Beim Klicken auf **Ändern** wird ein Fenster geöffnet, in dem Sie einen Prozesspfad ändern können. Kaspersky Endpoint Security schließt die angegebenen Prozesse aus der Untersuchung von Speichern aus.

Wenn Sie auf die Schaltfläche **Hinzufügen** klicken, wird ein Fenster geöffnet, in dem Sie den vollständigen Pfad des Prozesses eingeben können. Kaspersky Endpoint Security schließt die angegebenen Prozesse aus der Untersuchung von Speichern aus.

Ausschlüsse in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie Untersuchungsausschlüsse für den Prozess-Speicher in den Richtlinieneigenschaften konfigurieren (**Allgemeine Einstellungen** → **Prozess-Speicher ausschließen**).

Durch Klicken auf die Schaltfläche **Konfigurieren** im Block **Prozess-Speicher von Untersuchung ausschließen** wird ein Fenster geöffnet, in dem Sie eine Liste mit Ausschlüssen erstellen können.

Die Liste im Fenster **Prozess-Speicher von der Untersuchung ausschließen** enthält Pfade zu Prozessen, die die App von der Untersuchung des Prozess-Speichers ausschließt. Bei der Angabe des Pfades können Sie Masken verwenden. Standardmäßig ist die Liste leer.

Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben.

Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst.

Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Sie können Elemente in der Liste hinzufügen, bearbeiten und löschen.

Bei einem Klick auf **Löschen** löscht Kaspersky Endpoint Security den ausgewählten Prozesspfad aus der Liste.

Diese Schaltfläche ist verfügbar, wenn in der Liste mindestens ein Prozesspfad ausgewählt ist.

Beim Klicken auf **Ändern** wird ein Fenster geöffnet, in dem Sie einen Prozesspfad ändern können. Kaspersky Endpoint Security schließt die angegebenen Prozesse aus der Untersuchung von Speichern aus.

Wenn Sie auf die Schaltfläche **Hinzufügen** klicken, wird ein Fenster geöffnet, in dem Sie den vollständigen Pfad des Prozesses eingeben können. Kaspersky Endpoint Security schließt die angegebenen Prozesse aus der Untersuchung von Speichern aus.

Ausschlüsse über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie Untersuchungsausschlüsse für den Prozess-Speicher mithilfe des Parameters `MemScanExcludedProgramPath.item_#` in den allgemeinen App-Einstellungen konfigurieren.

Sie können den Wert des Parameters mithilfe von Befehlszeilenschaltern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen App-Einstellungen enthält.

Der Parameter `MemScanExcludedProgramPath.item_#` enthält den vollständigen Pfad zum Prozess im lokalen Verzeichnis. Bei der Angabe des Pfades können Sie Masken verwenden.

Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Sie können mehrere Prozesse angeben, die von der Untersuchung ausgeschlossen werden sollen.

Modus des Moduls zum Abfangen von Dateioperationen auswählen

Der Modus des Moduls zum Abfangen von Dateioperationen hat Auswirkungen auf die Ausführung der Komponenten Schutz vor bedrohlichen Dateien und Gerätekontrolle.

- Die App kann den Zugriff auf Dateien blockieren, die während der Untersuchung der Komponente "Schutz vor bedrohlichen Dateien" geprüft werden. Der Zugriff ist standardmäßig blockiert: Jeder Zugriff auf eine zu untersuchende Datei wartet auf das Resultat der Untersuchung. Wenn die Untersuchung in der Datei keine Bedrohungen erkennt, erlaubt die App den Zugriff auf die Datei. Wenn infizierte Objekte gefunden werden, führt die App die in den Einstellungen der Komponente "Schutz vor bedrohlichen Dateien" angegebene **Erste Aktion** (`FirstAction`) und **Zweite Aktion** (`SecondAction`) aus.

  Sie können das Blockieren des Zugriffs auf Dateien, die von der Komponente "Schutz vor bedrohlichen Dateien" untersucht werden, deaktivieren. In diesem Fall erfolgt die Untersuchung asynchron.

- Die App kann den Zugriff auf Dateien auf einem Gerät blockieren, während Gerätekontrolle bestimmt, ob der Zugriff auf das Gerät gewährt werden kann. Der Zugriff ist standardmäßig blockiert: Jeder Dateizugriff auf dem kontrollierten Gerät wartet auf das Resultat der Untersuchung. Die App gewährt den Zugriff auf Dateien, wenn aufgrund des Untersuchungsergebnisses der Gerätekontrolle der Zugriff auf das Gerät mit den Dateien erlaubt ist.

  Sie können das Blockieren des Zugriffs auf Dateien auf einem Gerät, das von der der Komponente "Gerätekontrolle" kontrolliert wird, deaktivieren. In diesem Fall bestimmt die Gerätekontrolle, ob ein Zugriff auf das Gerät möglich ist, asynchron.

Konfiguration in der Web Console

In der Web Console können Sie den Modus des Moduls zum Abfangen von Dateioperationen in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen** → **Allgemeine Einstellungen** → **App-Einstellung**, Abschnitt **Modus des Moduls zum Abfangen von Dateioperationen**).

Das Kontrollkästchen **Zugriff auf Dateien während der Untersuchung blockieren** aktiviert oder deaktiviert den Zugriff auf Dateien während der Untersuchung durch die Komponenten "Schutz vor bedrohlichen Dateien" und "Gerätekontrolle".

Das Kontrollkästchen ist standardmäßig aktiviert.

Wenn das Kontrollkästchen deaktiviert ist, ist der Zugriff auf jede Datei während der Untersuchung zulässig und die Untersuchung wird im asynchronen Modus durchgeführt.

Konfiguration in der Verwaltungskonsole

In der Verwaltungskonsole können Sie den Modus des Moduls zum Abfangen von Dateioperationen in den Richtlinieneigenschaften konfigurieren (**Allgemeine Einstellungen** → **App-Einstellung**, Abschnitt **Modus des Moduls zum Abfangen von Dateioperationen**).

Das Kontrollkästchen **Zugriff auf Dateien während der Untersuchung blockieren** aktiviert oder deaktiviert den Zugriff auf Dateien während der Untersuchung durch die Komponenten "Schutz vor bedrohlichen Dateien" und "Gerätekontrolle".

Das Kontrollkästchen ist standardmäßig aktiviert.

Wenn das Kontrollkästchen deaktiviert ist, ist der Zugriff auf jede Datei während der Untersuchung zulässig und die Untersuchung wird im asynchronen Modus durchgeführt.

Konfiguration über die Befehlszeile

Über die Befehlszeile können Sie den Modus des Moduls zum Abfangen von Dateioperationen mithilfe des Parameters `FileBlockDuringScan` in den allgemeinen Einstellungen der Anwendung konfigurieren.

Sie können den Wert des Parameters mithilfe von Befehlszeilenschaltern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen App-Einstellungen enthält.

Der Parameter `FileBlockDuringScan` kann die folgenden Werte annehmen:

- `Ja` (Standardwert) – blockiert den Zugriff auf Dateien während der Untersuchung durch die Komponenten "Schutz vor bedrohlichen Dateien" und "Gerätekontrolle".
- `Nein` – blockiert den Zugriff auf Dateien während der Untersuchung nicht. Der Zugriff auf eine beliebige Datei ist erlaubt, die Überprüfung erfolgt im asynchronen Modus.

  Dieser Modus des Moduls zum Abfangen von Dateioperationen hat während der Ausführung weniger Auswirkungen auf die Systemleistung. Es besteht jedoch das Risiko, dass eine Bedrohung in einer Datei nicht desinfiziert oder entfernt wird, wenn diese Datei beispielsweise während der Untersuchung ihren Namen ändert, bevor die App eine Entscheidung über den Status dieser Datei treffen kann.

Erkennen von Anwendungen konfigurieren, die von Angreifern für Kompromittierungen ausgenutzt werden können

Aktivieren und deaktivieren Sie die Erkennung von legitimen Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können.

Konfiguration in der Web Console

In der Web Console können Sie die Erkennung legitimer Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können in den Richtlinieneinstellungen aktivieren und deaktivieren (**App-Einstellungen** → **Allgemeine Einstellungen** → **App-Einstellungen**, Abschnitt **Untersuchungseinstellungen**).

Das Kontrollkästchen **Erkennung legitimer Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können** aktiviert oder deaktiviert die Erkennung legitimer Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Konfiguration in der Verwaltungskonsole

In der Verwaltungskonsole können Sie die Erkennung legitimer Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können in den Richtlinieneinstellungen aktivieren und deaktivieren (**Allgemeine Einstellungen** → **App-Einstellungen**, Abschnitt **Untersuchungseinstellungen**).

Das Kontrollkästchen **Erkennung legitimer Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können** aktiviert oder deaktiviert die Erkennung legitimer Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Konfiguration über die Befehlszeile

Über die Befehlszeile können Sie die Erkennung legitimer Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können, mithilfe des Parameters `DetectOtherObjects` in den allgemeinen App-Einstellungen aktivieren und deaktivieren.

Sie können den Wert des Parameters mithilfe von Befehlszeilenschaltern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen App-Einstellungen enthält.

Der Parameter `DetectOtherObjects` kann die folgenden Werte annehmen:

- `Yes` – Aktiviert die Erkennung legitimer Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können.
- `No` – Aktiviert nicht die Erkennung legitimer Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können.

Überwachung der Anwendungsstabilität aktivieren

Sie können der Überwachung der Anwendungsstabilität von Kaspersky Endpoint Security aktivieren oder deaktivieren, mit der Sie die Anzahl der ungeplanten Unterbrechungen der App verfolgen und den Administrator über den instabilen Betrieb der App informieren können.

Konfiguration in der Web Console

In der der Web Console können Sie die Überwachung der Anwendungsstabilität in den Richtlinieneigenschaften aktivieren oder deaktivieren (**App-Einstellungen** → **Allgemeine Einstellungen** → **App-Einstellungen**, Abschnitt **Erweiterte App-Einstellungen**).

Das Kontrollkästchen **Überwachung der Anwendungsstabilität aktivieren** aktiviert oder deaktiviert die Überwachung der Anwendungsstabilität von Kaspersky Endpoint Security.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Um die Einstellungen zu übernehmen, muss die App neu gestartet werden.

Wenn die App instabil läuft, wird in den Eigenschaften des Geräts mit der installierten App die folgende Meldung angezeigt: *<Anzahl> ungeplanter Unterbrechungen der App seit <Datum und Uhrzeit>*.

Konfiguration in der Verwaltungskonsole

In der der Verwaltungskonsole können Sie die Überwachung der Anwendungsstabilität in den Richtlinieneigenschaften aktivieren oder deaktivieren (**Allgemeine Einstellungen** → **App-Einstellungen**, Abschnitt **Erweiterte App-Einstellungen**).

Das Kontrollkästchen **Überwachung der Anwendungsstabilität aktivieren** aktiviert oder deaktiviert die Überwachung der Anwendungsstabilität von Kaspersky Endpoint Security.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Um die Einstellungen zu übernehmen, muss die App neu gestartet werden.

Wenn die App instabil läuft, wird in den Eigenschaften des Geräts mit der installierten App die folgende Meldung angezeigt: *<Anzahl> ungeplante Unterbrechungen der App seit <Datum und Uhrzeit>*.

Konfiguration über die Befehlszeile

In der Befehlszeile können Sie die Überwachung der Anwendungsstabilität mithilfe der Parameter `TrackProductCrashes`, `ProductHealthLogFile`, `WarnThreshold`, `WarnAfter_#_crash` und `WarnRemovingThreshold` in der Konfigurationsdatei kesl.ini konfigurieren.

Mit dem Parameter `TrackProductCrashes` können Sie die Überwachung der Anwendungsstabilität aktivieren oder deaktivieren. Der Parameter kann die folgenden Werte annehmen:

- `Yes/true` – Überwachung der Anwendungsstabilität aktivieren
- `No/false` – Überwachung der Anwendungsstabilität nicht aktivieren

Mit dem Parameter `ProductHealthLogFile` können Sie den Pfad zu der Datei angeben, die zur Überwachung der Anwendungsstabilität verwendet wird. Standardwert: /var/opt/kaspersky/kesl/private/kesl_health.log.

Mit dem Parameter `WarnThreshold` können Sie das Zeitintervall (in Sekunden) angeben, in dem die App die Anzahl der ungeplanten Unterbrechungen zählen soll, bevor eine Warnung über Instabilität angezeigt wird. Standardwert: 3600 Sekunden

Mit dem Parameter `WarnRemovingThreshold` können Sie das Zeitintervall (in Sekunden) festlegen, nach dem der Status "Instabil" der App entfernt wird. Standardwert: 86400 Sekunden

Mit dem Parameter `WarnAfter_#_crash` können Sie die Anzahl der ungeplanten Unterbrechungen der App festlegen, die erforderlich sind, um eine Benachrichtigung über eine instabile Ausführung der App anzuzeigen. Der Parameter kann die Werte 0 bis 10 annehmen. Standardwert: 10. Wenn der Wert auf 0 gesetzt ist, wird die keine Benachrichtigung über die Anwendungsinstabilität angezeigt.

Starteinstellungen der App konfigurieren

Sie können die Starteinstellungen der App konfigurieren.

Begrenzung in der Web Console konfigurieren

In der Web Console können Sie die Starteinstellungen der App in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen** → **Allgemeine Einstellungen** → **App-Einstellungen**, Abschnitt **Starteinstellungen der App**).

Starteinstellungen der Anwendung

Einstellung	Beschreibung
Maximale Anzahl an Wiederholungen für fehlgeschlagene Startversuche der Anwendung	Eingabefeld für die maximale Anzahl an Wiederholungen für fehlgeschlagene Startversuche der Anwendung. Standardwert: 5.
Maximale Wartezeit für den Anwendungsstart (Min.)	Eingabefeld für die maximale Wartezeit auf den Start der App (in Minuten), nach deren Überschreitung der Prozess "kesl" neu gestartet wird. Standardwert: 3.

Begrenzung in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Starteinstellungen der App in den Richtlinieneigenschaften konfigurieren (**Allgemeine Einstellungen** → **App-Einstellungen**, Abschnitt **Starteinstellungen der App**).

Wenn Sie im Block **Starteinstellungen für die App** auf die Schaltfläche **Konfigurieren** klicken, wird das Fenster **Starteinstellungen für die App** geöffnet, in dem Sie die Einstellungen für den Start der App konfigurieren können (siehe Tabelle unten).

Starteinstellungen der Anwendung

Einstellung	Beschreibung
Maximale Anzahl an Wiederholungen für fehlgeschlagene Startversuche der Anwendung	Eingabefeld für die maximale Anzahl an Wiederholungen für fehlgeschlagene Startversuche der Anwendung. Standardwert: 5.
Maximale Wartezeit für den Anwendungsstart (Min.)	Eingabefeld für die maximale Wartezeit auf den Start der App (in Minuten), nach deren Überschreitung der Prozess "kesl" neu gestartet wird. Standardwert: 3.

Begrenzung über die Befehlszeile konfigurieren

In der Befehlszeile können Sie Starteinstellungen der App mithilfe der Parameter `MaxRestartCount` und `StartupTimeout` in der Konfigurationsdatei kesl.ini konfigurieren.

Mit dem Parameter `MaxRestartCount` können Sie die maximale Anzahl erfolgloser aufeinanderfolgender Versuche zum Starten der App festlegen. Der Parameter kann die Werte 10 bis 100 annehmen. Standardwert: 5.

Mit dem Parameter `StartupTimeout` können Sie die maximale Wartezeit (in Minuten) auf den Start der App festlegen, nach deren Überschreitung der Prozess "kesl" neu gestartet wird. Der Parameter kann die Werte 10 bis 60 annehmen. Standardwert: 3.

Begrenzung der verwendeten Speicher- und CPU-Ressourcen

Sie können eine Begrenzung der Nutzung von CPU-Ressourcen für Untersuchungsaufgaben konfigurieren. Standardmäßig ist keine Begrenzung festgelegt. Sie können außerdem eine Begrenzung für die Speichernutzung der Untersuchungsaufgaben konfigurieren. Das Standardlimit beträgt 8192 MB.

Begrenzung in der Web Console konfigurieren

In der Web Console können Sie das Aktivieren und Deaktivieren der Begrenzung von CPU-Ressourcen sowie die Begrenzung für die Speichernutzung der Untersuchungsaufgaben in den Richtlinieneinstellungen konfigurieren (**App-Einstellungen** → **Allgemeine Einstellungen** → **App-Einstellungen**, Abschnitt **Leistung**).

Einstellungen

Einstellung	Beschreibung
Begrenzung der Speichernutzung für Untersuchungsaufgaben (MB)	Eingabefeld zur Begrenzung für die Speichernutzung der Untersuchungsaufgaben (in MB). Standardwert: 8192.
CPU-Ressourcen für Untersuchungsaufgaben begrenzen	Das Kontrollkästchen aktiviert oder deaktiviert die Begrenzung der CPU-Ressourcen für die Aufgaben "Untersuchung auf Malware", "Untersuchung wichtiger Bereiche", "Inventarisierung" und "Untersuchung von Containern". Wenn das Kontrollkästchen aktiviert ist, wird bei der Ausführung dieser Aufgaben die maximale Belastung aller CPU-Kerne den angegebenen Wert im Feld **Maximale Auslastung (%)** nicht überschreiten. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Begrenzung in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie das Aktivieren und Deaktivieren der Begrenzung von CPU-Ressourcen sowie die Begrenzung für die Speichernutzung der Untersuchungsaufgaben in den Richtlinieneinstellungen konfigurieren (**Allgemeine Einstellungen** → **App-Einstellungen**, Abschnitt **Leistung**).

Wenn Sie im Block **Leistung** auf die Schaltfläche **Konfigurieren** klicken, wird das Fenster **Ressourcenverbrauch für Prozessor und Speicher** geöffnet, in dem Sie Einschränkungen konfigurieren können (siehe Tabelle unten).

Einstellungen

Einstellung	Beschreibung
CPU-Ressourcen für Untersuchungsaufgaben	Das Kontrollkästchen aktiviert oder deaktiviert die Begrenzung der CPU-Ressourcen für die Aufgaben "Untersuchung auf Malware", "Untersuchung

begrenzen (%)	wichtiger Bereiche", "Inventarisierung" und "Untersuchung von Containern". Wenn das Kontrollkästchen aktiviert ist, wird bei der Ausführung dieser Aufgaben die maximale Belastung aller CPU-Kerne den angegebenen Wert im Feld rechts (in Prozent) nicht überschreiten. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Begrenzung der Speichernutzung für Untersuchungsaufgaben (MB)	Eingabefeld zur Begrenzung für die Speichernutzung der Untersuchungsaufgaben (in MB). Standardwert: 8192.

Begrenzung über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Begrenzung der Nutzung von CPU-Ressourcen für die Aufgaben vom Typ *ODS*, *ContainerScan* und *InventoryScan* mithilfe der Parameter `UseOnDemandCPULimit` und `OnDemandCPULimit` in den allgemeinen App-Einstellungen konfigurieren.

Sie können den Wert von Parametern mithilfe von Befehlszeilenschaltern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen App-Einstellungen enthält.

Der Parameter `UseOnDemandCPULimit` kann die folgenden Werte annehmen:

- `Yes` – Aktiviert die Begrenzung der Nutzung von CPU-Ressourcen für die Aufgabentypen *ODS*, *ContainerScan* und *InventoryScan*.
- `No` – Deaktiviert die Begrenzung der Nutzung von CPU-Ressourcen für Aufgaben.

Mit dem Parameter `OnDemandCPULimit` können Sie die maximale Auslastung aller Prozessorkerne (in Prozent) bei der Ausführung der Aufgabentypen *ODS*, *ContainerScan* und *InventoryScan* angeben. Der Parameter kann Werte von 10 bis 100 annehmen. Der Standardwert ist 100.

Über die Befehlszeile können Sie die Begrenzung der Speichernutzung für die Aufgaben vom Typ *ODS*, *ContainerScan* und *InventoryScan* mithilfe des Parameters `ScanMemoryLimit` in der Konfigurationsdatei kesl.ini konfigurieren. Standardwert: 8192.

Begrenzung des von der App verwendeten residenten Speichers

Sie können für die App eine Begrenzung des verwendeten residenten Speichers konfigurieren. Standardmäßig wird die Begrenzung automatisch festgelegt.

Begrenzung in der Web Console konfigurieren

In der Web Console können Sie für die App die Begrenzung des verwendeten residenten Speichers in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen** → **Allgemeine Einstellungen** → **App-Einstellungen**, Abschnitt **Erweiterte App-Einstellungen**).

Wenn Sie im Abschnitt **Erweiterte App-Einstellungen** auf den Link **Speichernutzung konfigurieren** klicken, wird ein Fenster geöffnet, in dem Sie die Begrenzung des verwendeten residenten Speichers konfigurieren können (siehe untere Tabelle).

Einstellungen

Einstellung	Beschreibung

Von der Anwendung genutzter residenter Speicher	In der Dropdown-Liste können Sie auswählen, auf welche Weise die Verwendung des residenten Speichers begrenzt werden soll: • **Unbegrenzt**. Wenn diese Option ausgewählt ist, wird die Verwendung des residenten Speichers nicht begrenzt. • **Grenzwert prozentual zur Gesamtgröße**. Bei Auswahl dieser Option wird das Feld **Speicherverwendung begrenzen auf (%)** verfügbar, in dem Sie den gewünschten Prozentwert angeben können. • **Grenzwert in Megabyte**. Wenn diese Option ausgewählt ist, wird das Feld **Speicherverwendung begrenzen auf (MB)** verfügbar, in dem Sie den gewünschten Wert in Megabyte angeben können. • **Kleineren der angegebenen Werte als Grenzwert (%, MB)**. Wenn Sie diese Option auswählen werden die Felder **Speicherverwendung begrenzen auf (%)** und **Speicherverwendung begrenzen auf (MB)** verfügbar, in denen Sie die gewünschten Werte angeben können. • **Größeren der angegebenen Werte als Grenzwert (%, MB)**. Wenn Sie diese Option auswählen werden die Felder **Speicherverwendung begrenzen auf (%)** und **Speicherverwendung begrenzen auf (MB)** verfügbar, in denen Sie die gewünschten Werte angeben können. • **Automatisch begrenzen (empfohlen)**. Wenn diese Option ausgewählt ist, wird die Verwendung des residenten Speichers automatisch begrenzt (Standardwert).
Begrenzung des genutzten Speichers (%)	Eingabefeld zur Begrenzung der Speichernutzung (in Prozent). Standardwert: 50.
Begrenzung des genutzten Speichers (MB)	Eingabefeld zur Begrenzung der Speichernutzung (in Megabyte). Standardwert: 2000.

Begrenzung in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie für die App die Beschränkung des verwendeten residenten Speichers den Richtlinieneigenschaften konfigurieren (**Allgemeine Einstellungen** → **App-Einstellungen**).

Wenn Sie im Abschnitt **Erweiterte App-Einstellungen** auf die Schaltfläche **Konfiguration** klicken, wird das Fenster **Erweiterte Einstellungen** geöffnet, in dem Sie die Begrenzung des verwendeten residenten Speichers konfigurieren können (siehe untere Tabelle).

Einstellungen

Einstellung	Beschreibung
Speichernutzung der Anwendung	In der Dropdown-Liste können Sie auswählen, auf welche Weise die Verwendung des residenten Speichers begrenzt werden soll: • **Unbegrenzt**. Wenn diese Option ausgewählt ist, wird die Verwendung des residenten Speichers nicht begrenzt. • **Automatisch begrenzen (empfohlen)**. Wenn Sie diese Option auswählen, wird die Verwendung des residenten Speichers automatisch begrenzt (Standardwert).

	• **Grenzwert prozentual zur Gesamtgröße**. Bei Auswahl dieser Option wird das Feld **Speicherverwendung begrenzen auf (%)** verfügbar, in dem Sie den gewünschten Prozentwert angeben können. • **Grenzwert in Megabyte**. Wenn diese Option ausgewählt ist, wird das Feld **Speicherverwendung begrenzen auf (MB)** verfügbar, in dem Sie den gewünschten Wert in Megabyte angeben können. • **Kleineren der angegebenen Werte als Grenzwert (%, MB)**. Wenn Sie diese Option auswählen werden die Felder **Speicherverwendung begrenzen auf (%)** und **Speicherverwendung begrenzen auf (MB)** verfügbar, in denen Sie die gewünschten Werte angeben können. • **Größeren der angegebenen Werte als Grenzwert (%, MB)**. Wenn Sie diese Option auswählen werden die Felder **Speicherverwendung begrenzen auf (%)** und **Speicherverwendung begrenzen auf (MB)** verfügbar, in denen Sie die gewünschten Werte angeben können.
Begrenzung des genutzten Speichers (%)	Eingabefeld zur Begrenzung der Speichernutzung (in Prozent). Standardwert: 50.
Begrenzung des genutzten Speichers (MB)	Eingabefeld zur Begrenzung der Speichernutzung (in Megabyte). Standardwert: 2000.

Begrenzung über die Befehlszeile konfigurieren

In der Befehlszeile können Sie für die App die Begrenzung des verwendeten residenten Speichers mithilfe des Parameters `MaxMemory` in der Konfigurationsdatei kesl.ini konfigurieren.

Der Parameter `MaxMemory` kann die folgenden Werte annehmen:

- `off` – Die Nutzung des residenten Speichers ist nicht beschränkt.
- `<Wert>%` – Die verfügbaren Werte liegen zwischen 1 und 100 Prozent der Speichergröße.
- `<Wert>MB` – Wert in Megabyte.
- `lowest/<Wert>%/<Wert>MB` – Der niedrigste Wert zwischen dem Prozentwert und dem Megabyte-Wert.
- `highest/<Wert>%/<Wert>MB` – Der höchste Wert zwischen dem Prozentwert und dem Megabyte-Wert.
- `auto` – bis zu 50% des verfügbaren Speichers, jedoch minimal 2 GB und maximal 16 GB.

Der Standardwert ist `auto`.

Begrenzung der Anzahl der Aufgaben zur benutzerdefinierten Untersuchung

Sie können die Anzahl der Aufgaben zur benutzerdefinierten Untersuchung, die ein nicht privilegierter Benutzer gleichzeitig auf einem Gerät ausführen kann, begrenzen. Es gibt keine Begrenzung für die Anzahl der Aufgaben, die ein Root-Benutzer ausführen kann.

Sie können die Begrenzung der Anzahl gleichzeitig ausgeführter benutzerdefinierter Untersuchungsaufgaben in der Befehlszeile mithilfe des Parameters `LimitNumberOfScanFileTasks` in den allgemeinen App-Einstellungen aktivieren und deaktivieren.

Sie können den Wert des Parameters mithilfe von Befehlszeilenschaltern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen App-Einstellungen enthält.

Der Parameter `LimitNumberOfScanFileTasks` kann Werte von 0 bis 4294967295 annehmen. Standardwert: 0.

Wenn der Wert 0 angegeben ist, kann ein nicht privilegierter Benutzer keine Aufgaben zur benutzerdefinierten Untersuchung starten.

Wenn Sie während der App-Installation das GUI-Paket installiert haben, wird für den Parameter `LimitNumberOfScanFileTasks` der Standardwert `5` verwendet.

Übertragung von Informationen an den Speicher von Kaspersky Security Center konfigurieren

In Kaspersky Security Center können Sie die Übertragung von Informationen über nicht verarbeitete Dateien und verbundene Geräte an den Speicher von Kaspersky Security Center aktivieren und deaktivieren.

Informationen zu nicht verarbeiteten Dateien werden in der Liste der aktiven Bedrohungen in Web Console (**Vorgänger → Speicher → Aktive Bedrohungen**) und in der Verwaltungskonsole (**Erweitert → Speicher → Aktive Bedrohungen**) angezeigt.

Informationen zu Geräten, die auf dem Client-Gerät installiert oder mit diesem verbunden sind, werden in der Liste der Geräte in Web Console (**Vorgänge → Speicher → Geräte**) und in der Verwaltungskonsole (**Erweitert → Speicher → Geräte**) angezeigt. Informationen werden übertragen, wenn die Gerätekontrolle aktiviert ist.

Übertragung von Informationen in der Web Console aktivieren und deaktivieren

In der Web Console können Sie die Übertragung von Informationen in den **Richtlinieneigenschaften** aktivieren und deaktivieren (App-Einstellungen → **Allgemeine Einstellungen → Speichereinstellungen**).

Einstellungen zur Übertragung von Informationen an den Kaspersky Security Center

Einstellung	Beschreibung
Informieren über nicht verarbeitete Dateien aktiviert/deaktiviert	Dieser Umschalter aktiviert und deaktiviert das Senden von Benachrichtigungen über die während der Untersuchung nicht verarbeiteten Dateien an den Administrationsserver. Der Schalter ist standardmäßig aktiviert.
Informieren über installierte Geräte aktiviert/deaktiviert	Dieser Umschalter aktiviert oder deaktiviert die Übertragung von Informationen über die auf dem verwalteten Client-Gerät installierten Geräte an den Administrationsserver. Der Schalter ist standardmäßig aktiviert.

Übertragung von Informationen in der Verwaltungskonsole aktivieren und deaktivieren

In der Verwaltungskonsole können Sie die Übertragung von Informationen in den Richtlinieneigenschaften aktivieren und deaktivieren (**Allgemeine Einstellungen → Speichereinstellungen**).

Einstellungen zur Übertragung von Informationen an den Kaspersky Security Center

Einstellung	Beschreibung
Über nicht verarbeitete Dateien informieren	Dieses Kontrollkästchen aktiviert und deaktiviert das Senden von Benachrichtigungen über die während der Untersuchung nicht verarbeiteten Dateien an den Administrationsserver. Das Kontrollkästchen ist standardmäßig aktiviert.
Über installierte Geräte informieren	Dieses Kontrollkästchen aktiviert oder deaktiviert die Übertragung von Informationen über die auf dem verwalteten Client-Gerät installierten Geräte an den Administrationsserver. Das Kontrollkästchen ist standardmäßig aktiviert.

Berechtigungen für die Aufgabenverwaltung konfigurieren

In Kaspersky Security Center können Sie die folgenden Berechtigungen für Benutzer konfigurieren:

- Berechtigung zum Anzeigen von Aufgaben, die in Kaspersky Endpoint Security erstellt wurden;
- Berechtigung zum Anzeigen von Aufgaben, die in Kaspersky Security Center auf Client-Geräten erstellt wurden.

Konfiguration in der Web Console

In der Web Console können Sie die Berechtigung zum Anzeigen von Aufgaben in den Richtlinieneinstellungen konfigurieren (**App-Einstellungen** → **Lokale Aufgaben** → **Aufgabenverwaltung**).

Einstellungen der Aufgabenverwaltung

Einstellung	Beschreibung
Benutzern das Anzeigen und Verwalten von lokalen Aufgaben erlauben	Dieses Kontrollkästchen erlaubt oder verbietet Benutzern, lokale, in der App Kaspersky Endpoint Security erstellte Aufgaben anzuzeigen und diese Aufgaben auf verwalteten Client-Geräten zu verwalten. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Benutzern das Anzeigen und Verwalten von Aufgaben erlauben, die in KSC erstellt wurden	Dieses Kontrollkästchen erlaubt bzw. verbietet den Benutzern die Anzeige von Aufgaben, die über die Kaspersky Security Center Web Console erstellt wurden, und die Verwaltung dieser Aufgaben auf verwalteten Client-Geräten. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Konfiguration in der Verwaltungskonsole

In der Verwaltungskonsole können Sie die Berechtigung zum Anzeigen von Aufgaben in den Richtlinieneinstellungen konfigurieren (**Lokale Aufgaben** → **Aufgabenverwaltung**).

Einstellungen der Aufgabenverwaltung

Einstellung	Beschreibung
Benutzern das Anzeigen und Verwalten von lokalen Aufgaben erlauben	Dieses Kontrollkästchen erlaubt oder verbietet Benutzern, lokale, in der App Kaspersky Endpoint Security erstellte Aufgaben anzuzeigen und diese Aufgaben auf verwalteten Client-Geräten zu verwalten.

	Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Benutzern das Anzeigen und Verwalten von Aufgaben erlauben, die in KSC erstellt wurden	Dieses Kontrollkästchen erlaubt oder verbietet Benutzern, über Kaspersky Security Center erstellte Aufgaben anzuzeigen und diese Aufgaben auf verwalteten Client-Geräten zu verwalten. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Backup

Wenn Kaspersky Endpoint Security während der Untersuchung eines geschützten Geräts bösartigen Code in einer Datei erkennt, kann die App die Datei blockieren, ihr den Status *Infiziert* zuweisen, eine Kopie davon im Backup ablegen und versuchen, die Datei zu desinfizieren.

Backup – Der Speicher der Backup-Kopien von Dateien, die gelöscht oder bei der Desinfektion verändert wurden.
Backup-Kopie – Die Kopie einer Datei, die vor der ersten Desinfektion oder vor dem Löschen dieser Datei erstellt wird. Die Backup-Kopien von Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

Wenn die Datei desinfiziert werden kann, ändert sich der Status der Backup-Kopie in *Desinfiziert*. Es kann vorkommen, dass Dateien bei der Desinfektion nicht vollständig erhalten bleiben. Wenn aufgrund einer Desinfektion wichtige Informationen, die in einer Datei enthalten waren, vollständig oder teilweise verloren gegangen sind, können Sie versuchen, die Datei aus ihrer desinfizierten Backup-Kopie im ursprünglichen Verzeichnis der Datei wiederherzustellen.

Es wird empfohlen, Dateien nur dann aus Backup-Kopien wiederherzustellen, wenn ihnen der Status *Desinfiziert* zugewiesen wurde. Die Wiederherstellung infizierter Objekte kann zu einer Infektion des Geräts führen.

Backup-Kopien von Dateien im Backup können personenbezogene Daten enthalten. Für den Zugriff auf die Objekte im Backup sind Root-Rechte erforderlich.

Sie können die folgenden Backup-Einstellungen konfigurieren:

- Speicherzeit von Objekten im Backup Standardmäßig werden Objekte 90 Tage lang gespeichert.
- Maximale Backup-Größe Standardmäßig ist die Größe des Backups unbegrenzt.
- Backup-Pfad Standardmäßig befindet sich das Backup im Verzeichnis /var/opt/kaspersky/kesl/common/objects-backup/.

Nach Ablauf der angegebenen Zeit oder bei Erreichen der maximalen Backup-Größe löscht die App automatisch Backup-Kopien von Dateien mit beliebigem Status aus dem Backup.

Sie können eine Backup-Kopie sowohl einer wiederhergestellten als auch einer nicht wiederhergestellten Datei auch selbst löschen.

Eine allgemeine Liste der Dateien, die von Kaspersky-Apps auf Client-Geräten im Backup abgelegt werden, wird in Kaspersky Security Center erstellt und ist in der Verwaltungskonsole (**Erweitert → Speicher → Backup**) und in der Web Console (**Vorgänge → Speicher → Backup**) verfügbar. Sie können die Eigenschaften von Dateien anzeigen, die sich im Backup auf geschützten Geräten befinden, eine Schadsoftware-Untersuchung im Backup durchführen und Dateien daraus löschen. Kaspersky Security Center kopiert keine Dateien vom Backup auf den Administrationsserver; alle Dateien werden im Backup auf geschützten Geräten abgelegt. Die Dateiwiederherstellung wird auf einem geschützten Gerät durchgeführt.

Backup-Einstellungen in der Web Console konfigurieren

In der Web Console können Sie die Backup-Einstellungen in den Richtlinieneinstellungen konfigurieren (**App-Einstellungen → Allgemeine Einstellungen → Speichereinstellungen**).

Einstellungen des Backup-Speichers

Einstellung	Beschreibung
Über Dateien im Backup-Speicher informieren aktiviert/deaktiviert	Dieser Schalter aktiviert oder deaktiviert den Versand von Benachrichtigungen über Dateien im Backup an den Administrationsserver. Der Schalter ist standardmäßig aktiviert.
Objekte nicht länger speichern als (Tage)	Eingabefeld zur Angabe des Zeitraums für das Speichern von Objekten im Backup. Zulässige Werte: 0–3653. Standardwert: 90. Ist der Wert 0 angegeben, dann ist der Zeitraum der Speicherung der Objekte im Backup nicht begrenzt.
Größe des Back-Speichers begrenzen auf (MB)	Eingabefeld zur Angabe der maximalen Backup-Größe (in Megabyte). Zulässige Werte: 0–999999. Standardwert: 0 (die Größe des Backups ist nicht begrenzt).

Backup-Einstellungen in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Backup-Einstellungen in den **Richtlinieneinstellungen** konfigurieren (Allgemeine Einstellungen → **Speichereinstellungen**).

Einstellungen des Backup-Speichers

Einstellung	Beschreibung
Über Dateien im Backup-Speicher informieren	Dieses Kontrollkästchen aktiviert oder deaktiviert den Versand von Benachrichtigungen über Dateien im Backup an den Administrationsserver. Das Kontrollkästchen ist standardmäßig aktiviert.
Objekte nicht länger speichern als (Tage)	Dieses Kontrollkästchen aktiviert oder deaktiviert die Begrenzung der Speicherdauer von Objekten im Backup um ein angegebenes Zeitintervall. Zulässige Werte: 0–3653. Standardwert: 90. Ist der Wert 0 angegeben, dann ist der Zeitraum der Speicherung der Objekte im Backup nicht begrenzt.
Größe des Back-Speichers begrenzen auf (MB)	Dieses Kontrollkästchen aktiviert oder deaktiviert die Begrenzung der maximalen Backup-Größe auf einen angegebenen Wert (in Megabyte). Zulässige Werte: 0–999999. Standardwert: 0 (die Größe des Backups ist nicht begrenzt).

Backup-Einstellungen über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Backup-Einstellungen mithilfe der vordefinierten Aufgabe "Backups-Verwaltung" (*Backup*) konfigurieren.

Die Aufgabe "Backup-Verwaltung" wird standardmäßig ausgeführt. Sie können diese Aufgabe nicht manuell starten und beenden.

Sie können die Backup-Einstellungen konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zur Backup-Verwaltung ändern.

Einstellungen der Aufgabe zur Backup-Verwaltung

Einstellung	Beschreibung	Wert
`DaysToLive`	Speicherzeit von Objekten im Backup (in Tagen) Um die Begrenzung der Speicherzeit von Objekten im Backup aufzuheben, geben Sie den Wert 0 an.	0 – Die Speicherzeit von Objekten im Backup ist nicht begrenzt. Standardwert: 90.
`BackupSizeLimit`	Maximale Backup-Größe (in Megabyte) Wenn die maximale Größe des Backups erreicht ist, löscht die App die ältesten Objekte. Um die Begrenzung der Backup-Größe aufzuheben, geben Sie den Wert 0 an.	0 – 999999 0 – Die Größe des Backups ist nicht begrenzt. Standardwert: 0.
`BackupFolder`	Pfad des Backup-Verzeichnisses Sie können ein benutzerdefiniertes Backup-Verzeichnis angeben, das sich vom Standardverzeichnis unterscheidet. Sie können für das Backup ein beliebiges Verzeichnis auf beliebigen Geräten wählen. Es wird nicht empfohlen, Verzeichnisse zu wählen, die sich auf Remote-Geräten befindet und etwa über Samba- oder NFS-Protokolle gemountet sind. Kaspersky Endpoint Security beginnt, die Objekte im angegebenen Verzeichnis zu speichern, sobald Sie die Einstellungen geändert und die App neu gestartet haben. Wenn das angegebene Verzeichnis nicht existiert oder nicht verfügbar ist, verwendet die App das Standardverzeichnis.	Standardwert: /var/opt/kaspersky/kesl/common/objects-backup/ Für den Zugriff auf das Standardverzeichnis für das Backup sind Root-Rechte erforderlich.

Verwendung von Objekten im Backup über die Befehlszeile

Über die Befehlszeile können Sie mit Befehlen zur Verwaltung des Backups die folgenden Aktionen mit Backup-Objekten ausführen:

- Informationen zu Backup-Objekten anzeigen.
- Alle oder nur bestimmte Objekte aus dem Backup löschen.
- Objekte aus dem Backup wiederherstellen.

Die Wiederherstellung infizierter Objekte kann zu einer Infektion des Geräts führen.

Informationen zu Backup-Objekten anzeigen

Um Informationen zu Backup-Objekten anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control -B --query ["<Filterbedingungen>"] [-n <Anzahl>] [--json]
```

Wobei gilt:

- `<Filterbedingungen>` – Ein oder mehrere logische Ausdrücke im Format `<Feld> <Vergleichsoperator> '<Wert>'`, kombiniert mit dem logischen Operator `and` zur Eingrenzung der Abfrageergebnisse. Wenn Sie keine Filterbedingungen angeben, zeigt die App Informationen zu allen Backup-Objekten an.
- `<Anzahl>` – Die Anzahl der letzten Objekte aus dem Backup, die ausgegeben werden müssen. Wenn Sie den Schalter `-n` nicht angeben, werden die letzten 30 Objekte ausgegeben. Um alle Objekte anzuzeigen, geben Sie den Wert 0 ein.
- `--json` – Gibt Daten im JSON-Format aus.

In der Zeile `ObjectId` wird die numerische ID angezeigt, die die App dem Objekt zugewiesen hat, als es im Backup abgelegt wurde. Diese ID wird verwendet, um Aktionen für ein Objekt auszuführen, z. B. beim Wiederherstellen oder Löschen eines Objekts aus dem Backup.

Objekte aus dem Backup wiederherstellen

So stellen Sie ein Objekt unter dem ursprünglichen Namen am ursprünglichen Speicherort wieder her:

```
kesl-control --restore <Objekt-ID>
```

Wobei gilt: `<Objekt-ID>` ist die numerische ID, die die App dem Objekt zugewiesen hat, als es im Backup abgelegt wurde.

So stellen Sie ein Objekt unter einem neuen Namen in einem angegebenen Verzeichnis wieder her:

```
kesl-control --restore <Objekt-ID> --file <Dateiname und Dateipfad>
```

Wobei gilt: `--file <Dateiname und Dateipfad>` – Der neue Dateiname und der Pfad zu dem Verzeichnis, in dem Sie die Datei speichern möchten. Wenn das angegebene Verzeichnis nicht existiert, wird es von der App erstellt.

Bestimmte Objekte aus dem Backup löschen

Um ausgewählte Objekte aus dem Backup zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control --mass-remove --query "<Filterbedingungen>"
```

`Wobei gilt: <Filterbedingungen>` – Ein oder mehrere logische Ausdrücke im Format `<Feld> <Vergleichsoperator> '<Wert>'`, kombiniert mit dem logischen Operator `and` zur Eingrenzung der Abfrageergebnisse.

Beispiele:
Um das Objekt mit ID=15 zu löschen:

```
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

So löschen Sie Objekte, deren Namen oder Pfade "test" enthalten:

```
kesl-control -B --mass-remove --query "FileName like '%test%'"
```

Um alle Objekte aus dem Backup zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control -B --mass-remove
```

Integration mit Detection and Response

Die Lösungen Detection and Response von Kaspersky sind Sicherheitssysteme, die darauf ausgelegt sind, komplexe Bedrohungen und Anzeichen von Angriffen auf verschiedenen Ebenen der Infrastruktur eines Unternehmens zu erkennen. Die Lösungen Detection and Response liefern Ihnen Informationen über erkannte Bedrohungen und ermöglichen Ihnen, Reaktionsmaßnahmen zu verwalten.

Kaspersky Endpoint Security kann mit den folgenden Lösungen Detection and Response von Kaspersky interagieren:

- Kaspersky Anti Targeted Attack Platform (Komponente von Kaspersky Endpoint Detection and Response). Die Integration mit Kaspersky Endpoint Detection and Response (KATA) erfolgt durch Kaspersky Endpoint Security – Endpoint Detection and Response (KATA) (im Weiteren auch "EDR (KATA)").

- Kaspersky Endpoint Detection and Response Optimum. Die Integration erfolgt durch Endpoint Detection and Response Optimum (im Weiteren auch "EDR Optimum").

- Managed Detection and Response. Die Integration erfolgt durch Kaspersky Endpoint Security – Managed Detection and Response (im Weiteren auch "MDR").

Im Rahmen der Integration von Kaspersky Endpoint Security mit den Lösungen Kaspersky Managed Detection and Response und Kaspersky Anti Targeted Attack Platform kann im systemd-Protokoll eine große Anzahl an Ereignissen eingetragen werden. Wenn Sie das Eintragen der Audit-Ereignisse in systemd deaktivieren wollen, müssen Sie den Socket systemd-journald-audit deaktivieren und das Betriebssystem neu starten.

So deaktivieren Sie den Socket systemd-journald-audit:

```
systemctl stop systemd-journald-audit.socket

systemctl disable systemd-journald-audit.socket

systemctl mask systemd-journald-audit.socket
```

Die Konfiguration des Dienstes "auditd" ist auf dem Betriebssystem SintezM-Client standardmäßig gegen Änderungen gesperrt, d. h. sie befindet sich im Ausführungsmodus `enabled 2`. Damit die Komponente "Verhaltensanalyse" bei einer Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response und Kaspersky Anti Targeted Attack Platform ordnungsgemäß funktioniert, müssen Sie in den Konfigurationsdateien den Ausführungsmodus von auditd in den Modus ohne Sperrung der Konfiguration (d. h. `enabled 1`) ändern und anschließend einen Neustart des Betriebssystems durchführen.

Antwort-Reaktionen auf Befehle von Detection and Response

Kaspersky Endpoint Security kann Antwort-Reaktionen ausführen, die zur Bereitstellung von Sicherheitsfunktionen vorgesehen sind:

- Während der Interaktion mit Kaspersky Anti Targeted Attack Platform – Kaspersky Endpoint Detection and Response (KATA).

- Während der Interaktion mit Kaspersky Endpoint Detection and Response Optimum.

Die Einstellungen der Antwort-Reaktionen von Kaspersky Anti Targeted Attack Platform und Kaspersky Endpoint Detection and Response Optimum unterscheiden sich voneinander.

Kaspersky Endpoint Security kann die folgenden Antwort-Reaktionen ausführen:

- Dateien vom Gerät abrufen.

  Die Aktion wird mithilfe der Aufgabe *Datei abrufen* (Get file task) ausgeführt. Beispielsweise können Sie das Abrufen einer Ereignisprotokoll-Datei konfigurieren, die von der Anwendung eines Drittanbieters generiert wird.

- Dateien von Geräten löschen.

  Die Aktion wird mithilfe der Aufgabe *Datei löschen* (Delete file task) ausgeführt.

- Prozesse auf Geräten remote starten.

  Die Aktion wird mithilfe der Aufgabe *Prozess starten* (Run process) ausgeführt.

  Sie können beispielsweise per Fernzugriff ein Tool starten, das eine Gerätekonfigurationsdatei erstellt, und diese Datei anschließend mittels der Aufgabe *Datei abrufen* abrufen.

- Prozesse auf Geräten remote beenden.

  Die Aktion wird mithilfe der Aufgabe *Prozess beenden* (Terminate process) ausgeführt.

  Sie können beispielsweise remote ein Tool zur Messung der Internet-Geschwindigkeitstest beenden, welches vorher mit der Aufgabe "Prozess starten" gestartet wurde.

- *Anzeichen einer Kompromittierung* von Geräten erkennen und mit einer Reaktion auf die Bedrohung reagieren.

  Die Aktion wird mithilfe der Aufgabe *IoC-Untersuchung* (IOC Scan) ausgeführt.

  Beim Ausführen der Aufgabe *IOC-Untersuchung* erfolgt die Prüfung anhand von IOC-Bewertungen (Eigenschaften eines IOC-Objekts, z. B. der Hash einer Datei) nur im Hauptnamensraum des Betriebssystems. Die Aufgabe *IOC-Untersuchung* berechnet keine Hashes für Dateien, die größer als 200 MB sind.

- Die Netzwerkisolation des Geräts aktivieren oder deaktivieren.

  Bei einer Interaktion zwischen Kaspersky Endpoint Security und Kaspersky Endpoint Detection and Response Optimum können Sie Folgendes tun:

  - Die Netzwerkisolation in der Web Console oder in der Kaspersky Security Center Cloud Console aktivieren oder deaktivieren.
  - Die Netzwerkisolation über die Befehlszeile deaktivieren .
  - Die automatische Deaktivierung der Netzwerkisolation in der Web Console oder in der Kaspersky Security Center Cloud Console konfigurieren.

  Bei einer Interaktion zwischen Kaspersky Endpoint Security und Kaspersky Endpoint Detection and Response (KATA) können Sie Folgendes tun:

  - Die Netzwerkisolation über die Befehlszeile deaktivieren .
  - Die Netzwerkisolation über Kaspersky Endpoint Detection and Response (KATA) aktivieren oder deaktivieren.

    Weitere Informationen zu der Lösung finden Sie in der Hilfe zu Kaspersky Anti Targeted Attack Platform.

Einschränkungen der Netzwerkisolation

Bei Verwendung der Netzwerkisolation wird dringend empfohlen, dass Sie sich mit den unten beschriebenen Einschränkungen vertraut machen.

Damit die Netzwerkisolation funktioniert, muss Kaspersky Endpoint Security ausgeführt werden. Bei einem Ausfall von Kaspersky Endpoint Security (d. h., wenn die App wird nicht ausgeführt) ist die Blockierung des Datenverkehrs bei aktivierter Netzwerkisolation durch Kaspersky Anti Targeted Attack Platform oder Kaspersky Endpoint Detection and Response Optimum nicht garantiert.

Während einer aktivierten Netzwerkisolation wird durchgeleiteter Datenverkehr (Transit) eingeschränkt unterstützt und kann gefiltert werden.

DHCP und DNS werden nicht automatisch zu den Ausnahmen der Netzwerkisolation hinzugefügt. Wenn also die Netzwerkadresse einer Ressource während der Netzwerkisolation geändert wurde, kann Kaspersky Endpoint Security nicht darauf zugreifen. Gleiches gilt für die Knoten eines fehlertoleranten KATA-Servers. Es wird nicht empfohlen, ihre Adressen zu ändern, damit Kaspersky Endpoint Security die Verbindung zu ihnen nicht verliert.

Proxy-Server werden nicht automatisch zu den Ausnahmen für die Netzwerkisolation hinzugefügt. Damit Kaspersky Endpoint Security die Verbindung zum KATA-Server nicht verliert, müssen Sie daher einen Proxy-Server manuell zu den Ausnahmen hinzufügen.

Das Hinzufügen zu und Ausschließen aus der Netzwerkisolation eines Prozesses anhand seines Namens wird nicht unterstützt.

Wenn Kaspersky Endpoint Security im Standard-Modus ausgeführt wird, werden bei Verwendung der Netzwerkisolation folgende Maßnahmen empfohlen:

- Verwendung des KSN-Proxy-Servers, um mit Kaspersky Security Network zu interagieren.
- Verwendung von Kaspersky Security Center als Proxy-Server, um die App zu aktivieren.

  Wenn es nicht möglich ist, Kaspersky Security Center als Proxy-Server zu verwenden, konfigurieren Sie die Einstellungen des erforderlichen Proxy-Servers und fügen Sie ihn zu den Ausnahmen hinzu.
- Verwendung von Kaspersky Security Center als Quelle für die Datenbankaktualisierungen.

Diese Empfehlungen gelten nicht, wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird.

Integration mit Kaspersky Managed Detection and Response (KATA)

Endpoint Detection and Response (KATA) ist eine Komponente der Kaspersky Anti Targeted Attack Platform. Die Integration mit Kaspersky Endpoint Detection and Response (KATA) erfolgt durch Kaspersky Endpoint Security – Endpoint Detection and Response (KATA) (im Weiteren auch "EDR (KATA)").

Kaspersky Endpoint Security unterstützt die Kaspersky Anti Targeted Attack Platform, die darauf ausgelegt ist, die IT-Infrastruktur einer Organisation zu schützen und Bedrohungen wie Zero-Day-Angriffe, zielgerichtete Angriffe und Advanced Persistent Threats (im Folgenden auch "APT") rechtzeitig zu erkennen. Weitere Informationen zu der Lösung finden Sie in der Hilfe zu Kaspersky Anti Targeted Attack Platform.

Diese Funktionalität wird im KESL-Container nicht unterstützt.

Im Rahmen der Interaktion mit Kaspersky Endpoint Detection and Response (KATA) kann Kaspersky Endpoint Security die folgenden Funktionen ausführen:

- Übertragen von Daten über Ereignisse auf Geräten (Telemetriedaten) an den Server von Kaspersky Anti Targeted Attack Platform mit der Komponente Central Node (im Folgenden auch "KATA-Server"). Kaspersky Endpoint Security sendet neben Überwachungsdaten zu Prozessen, offenen Netzwerkverbindungen und geänderten Dateien auch Daten zu den von der App erkannten Bedrohungen und zu den Verarbeitungsergebnissen dieser Bedrohungen an den KATA-Server.

- Ausführen von Reaktionsmaßnahmen, um die Sicherheitsfunktionen mittels der Befehle sicherzustellen, die von Kaspersky Anti Targeted Attack Platform übertragen wurden.

Für eine Integration mit Kaspersky Endpoint Detection and Response (KATA) muss die Komponente Verhaltensanalyse aktiviert sein.

Die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response (KATA) ist nur bei aktivierter Komponente "Verhaltensanalyse" möglich. Andernfalls werden die notwendigen Telemetriedaten nicht übertragen.

Darüber hinaus kann Kaspersky Endpoint Detection and Response (KATA) Daten verwenden, die es von den folgenden Komponenten abruft:

- Schutz vor bedrohlichen Dateien.

- Schutz vor Netzwerkbedrohungen.

- Schutz vor Web-Bedrohungen.

Während der Integration mit Kaspersky Endpoint Detection and Response (KATA) stellen Geräte mit Kaspersky Endpoint Security über das HTTPS-Protokoll sichere Verbindungen mit dem KATA-Server her. Um die Sicherheit dieser Verbindung zu gewährleisten, werden die folgenden, vom KATA-Server ausgestellten, Zertifikate verwendet:

- Zertifikat des KATA-Servers. Die Verbindung wird mit dem TLS-Zertifikat des Servers verschlüsselt. Sie können die Sicherheit der Verbindung erhöhen, indem Sie in Kaspersky Endpoint Security die Überprüfung des Serverzertifikats aktivieren. Dafür müssen Sie vor dem Aktivieren der Integration mit Kaspersky Endpoint Detection and Response (KATA) das Zertifikat des Integrationsservers hinzufügen.

- Client-Zertifikat. Dieses Zertifikat dient dem zusätzlichen Schutz der Verbindung durch Zwei-Wege-Authentifizierung (Überprüfung der Geräte mit dem KATA-Server von Kaspersky Endpoint Security). Mehrere Geräte können dasselbe Client-Zertifikat verwenden. Standardmäßig überprüft der KATA-Server keine Client-Zertifikate, aber die Zwei-Wege-Authentifizierung kann auf der Seite von Kaspersky Anti Targeted Attack Platform aktiviert werden. In diesem Fall müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen für die Integration mit Kaspersky Endpoint Detection and Response (KATA) aktivieren und ein Client-Zertifikat hinzufügen (ein Crypto-Container mit einem Zertifikat und einem privaten Schlüssel).

Die Zertifikate zur Sicherung der Verbindung zum KATA-Server werden vom Administrator der Kaspersky Anti Targeted Attack Platform bereitgestellt.

Wenn in den allgemeinen Einstellungen von Kaspersky Endpoint Security die Verwendung eines Proxy-Servers konfiguriert ist, wird für die Verbindung zum KATA-Server ein Proxy-Server verwendet.

Standardmäßig ist die Integration mit Kaspersky Endpoint Detection and Response (KATA) deaktiviert. Sie können die Integration aktivieren und deaktivieren und die folgenden Einstellungen für die Integration über die Befehlszeile, in der Web Console und mithilfe der Verwaltungskonsole konfigurieren:

- Konfigurieren Sie allgemeine Einstellungen für die Verbindung mit den KATA-Servern.

- Fügen Sie Zertifikate der KATA-Server hinzu und entfernen Sie sie.
- Konfigurieren Sie die Zwei-Wege-Authentifizierung beim Herstellen einer Verbindung mit den KATA-Servern und fügen Sie Client-Zertifikate hinzu.
- Konfigurieren Sie die Einstellungen zum Senden von Ereignissen.
- Aktivieren und deaktivieren Sie das Senden von Telemetriedaten.

  Wenn die Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response aktiviert ist, werden beim Senden von Telemetriedaten keine Ausschlüsse nach Prozess angewendet.

Das Verwalten der Einstellungen für die Integration mit Kaspersky Endpoint Detection and Response (KATA) über die Kaspersky Security Center Cloud Console wird nicht unterstützt.

Integration mit Kaspersky Endpoint Detection and Response (KATA) in der Web Console einrichten

In der Web Console können Sie die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response (KATA) aktivieren oder deaktivieren und Integrationseinstellungen den Richtlinieneinstellungen konfigurieren (**App-Einstellungen** → **Detection and Response** → **Endpoint Detection and Response (KATA)**).

Das Verwalten der Einstellungen für die Integration mitKaspersky Endpoint Detection and Response (KATA) über die Kaspersky Security Center Cloud Console wird nicht unterstützt.

Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA)

Einstellung	Beschreibung
Endpoint Detection and Response (KATA) ist aktiviert/deaktiviert	Aktiviert oder Deaktiviert die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response (KATA). Die Integration ist standardmäßig deaktiviert.
Einstellungen für die Verbindung mit dem Server	Wenn Sie auf den Link **Konfigurieren** klicken, wird ein Fenster geöffnet, in dem Sie bei Verbindung mit den KATA-Servern die allgemeinen Einstellungen für die Verbindung mit den KATA-Servern konfigurieren, ein Serverzertifikat hinzufügen und die Zwei-Wege-Authentifizierung konfigurieren können.
KATA-Server	Die Tabelle enthält eine Liste der KATA-Server, mit denen eine Verbindung konfiguriert ist. Durch Klicken auf die Schaltfläche **Hinzufügen** öffnet sich ein Fenster, in dem Sie die Verbindung zu einem KATA-Server konfigurieren können. Mit den Schaltflächen oberhalb der Tabelle können Sie bereits konfigurierte Verbindungseinstellungen ändern und löschen.
Maximale Verzögerung beim Versenden von Ereignissen (Sek.)	Maximale Verzögerung beim Senden von Ereignissen an den KATA-Server in Sekunden. Der Standardwert ist `30`.
Begrenzung für die	Aktiviert oder deaktiviert die Beschränkung der Anzahl an Ereignissen, die an den

Anzahl an Ereignissen aktivieren	KATA-Server gesendet werden.
Maximale Anzahl an Ereignissen pro Stunde	Die maximale Anzahl an Ereignissen innerhalb einer Stunde. Der Standardwert ist `3000`.
Maximale Anzahl an Ereignissen eines Typs in Prozent	Maximale Anzahl an Ereignissen eines Typs in Prozent. Die Übertragung von Ereignissen wird begrenzt, wenn das Verhältnis von Ereignissen des gleichen Typs (z. B. Änderung der Registrierung) zur Gesamtzahl der Ereignisse die prozentuale Grenze überschreitet. Der Standardwert ist `15`.

Fenster zum Konfigurieren der Verbindungseinstellungen mit den Servern

In diesem Fenster können Sie bei Verbindung mit den KATA-Servern die allgemeinen Einstellungen für die Verbindung mit den KATA-Servern konfigurieren, ein Serverzertifikat hinzufügen und die Zwei-Wege-Authentifizierung konfigurieren können.

Einstellungen der Verbindung mit dem KATA-Server

Einstellung	Beschreibung
Synchronisationsanfrage an den KATA-Server senden alle (Min.)	Häufigkeit des Sendens von Synchronisierungsanfragen an den KATA-Server in Minuten. Der Standardwert ist `5`.
Maximale Wartezeit für den Verbindungsaufbau mit einem Server (Sek.)	Die maximale Wartezeit auf eine Verbindung mit dem KATA-Server in Sekunden. Der Standardwert ist `10`.
Maximale Wartezeit für eine Serverantwort (Sek.)	Die maximale Wartezeit auf eine Antwort vom KATA-Server in Sekunden. Der Standardwert ist `10`.
Übertragung von Telemetriedaten erlauben	Aktiviert und deaktiviert des Sendens von Daten über Ereignisse auf Geräten (Telemetriedaten) an den KATA-Server. Standardmäßig ist das Senden von Telemetriedaten aktiviert.
Serverzertifikat	Nach dem Hinzufügen des Serverzertifikats werden die Informationen zum Zertifikat angezeigt: • Seriennummer des Zertifikats • Zertifikatinhaber • Zertifikataussteller • Beginn der Gültigkeitsdauer des Zertifikats • Ende der Gültigkeitsdauer des Zertifikats
Auswählen	Öffnet ein Standard-Dateiauswahlfenster, in welchem Sie den Pfad zum Zertifikat des KATA-Servers angeben können.

	Wenn ein Serverzertifikat hinzugefügt wird, überprüft Kaspersky Endpoint Security das Serverzertifikat, um die Sicherheitsstufe der Verbindung zu erhöhen.
Löschen	Entfernt ein zuvor hinzugefügtes Serverzertifikat. Diese Schaltfläche wird nur dann angezeigt, wenn ein Serverzertifikat hinzugefügt wurde.
Erweiterter Schutz der Verbindung	In diesem Einstellungsbereich können für die Verbindung mit einem KATA-Server die Zwei-Wege-Authentifizierung aktivieren oder deaktivieren und ein Client-Zertifikat hinzufügen.
Zwei-Wege-Authentifizierung verwenden	Aktiviert oder deaktiviert die Verwendung der Zwei-Wege-Authentifizierung für eine zusätzliche Absicherung der Verbindung zum KATA-Server. Auf der Seite des KATA-Servers muss die bidirektionale Authentifizierung aktiviert sein. Um die bidirektionale Authentifizierung zu verwenden, müssen Sie ein Client-Zertifikat hinzufügen.
Client-Zertifikat hinzufügen	Öffnet ein Standard-Dateiauswahlfenster, in dem Sie den Pfad zum Crypto-Container (Archiv im pfx-Format) mit dem Client-Zertifikat und dem privaten Schlüssel angeben können. Die Schaltfläche ist dann verfügbar, wenn das Kontrollkästchen **Zwei-Wege-Authentifizierung verwenden** aktiviert ist.
Bearbeiten	Ermöglicht die Angabe eines Kennworts für den Crypto-Container mit dem Client-Zertifikat. Das Feld **Kennwort des Crypto-Containers** kann nicht bearbeitet werden. Standardmäßig ist das Kennwort leer. Um ein Kennwort anzugeben, klicken Sie auf die Schaltfläche **Bearbeiten**, geben Sie im sich öffnenden Fenster das Kennwort ein und klicken Sie auf die Schaltfläche **OK**. Wenn Sie im Fenster zur Kennworteingabe auf die Schaltfläche **Anzeigen** klicken, wird das Kennwort im Klartext angezeigt. Es wird empfohlen, sicherzustellen, dass die Passwortkomplexität und die Anti-Brute-Force-Mechanismen gewährleisten, dass das Passwort innerhalb von 6 Monaten nicht geknackt werden kann. Die Schaltfläche ist dann verfügbar, wenn das Kontrollkästchen **Zwei-Wege-Authentifizierung verwenden** aktiviert ist.

Fenster zum Hinzufügen von Parametern für die Verbindung mit dem KATA-Server

In diesem Fenster können Sie die Parameter für die Verbindung zum KATA-Server festlegen.

Einstellungen der Verbindung mit dem KATA-Server

Einstellung	Beschreibung
Adresse	Adresse des KATA-Servers. Sie können die IP-Adresse (IPv4 oder IPv6) oder den vollqualifizierten Domänennamen (FQDN) des Servers angeben.

	Um sicherzustellen, dass die Kommunikation mit dem KATA-Server nicht unterbrochen wird, wenn die App bei aktivierter Netzwerkisolation des Geräts ausfällt, wird es empfohlen, die IP-Adresse des Servers anzugeben. Der Standardwert ist `127.0.0.1`.
Port	Port für die Verbindung zum KATA-Server. Der Standardwert ist `443`.

Integration mit Kaspersky Endpoint Detection and Response (KATA) in der Verwaltungskonsole einrichten

In Verwaltungskonsole können Sie die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response (KATA) aktivieren oder deaktivieren und die Integrationseinstellungen den Richtlinieneinstellungen konfigurieren (**Detection and Response → Endpoint Detection and Response (KATA)**).

Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA)

Einstellung	Beschreibung
Integration mit Endpoint Detection and Response (KATA)	Aktiviert oder Deaktiviert die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response (KATA). Die Integration ist standardmäßig deaktiviert.
KATA-Server	Wenn Sie auf die Schaltfläche **Konfigurieren** klicken, wird das Fenster **KATA-Server** geöffnet. In diesem Fenster können Sie die Verbindungen zu den KATA-Servern konfigurieren und die Liste der Server anzeigen, für welche die Verbindungen konfiguriert sind.
Einstellungen für die Verbindung mit dem Server	Wenn Sie auf die Schaltfläche **Konfigurieren** klicken, wird ein Fenster geöffnet, in dem Sie bei Verbindung mit den KATA-Servern die allgemeinen Einstellungen für die Verbindung mit den KATA-Servern konfigurieren, ein Serverzertifikat hinzufügen und die Zwei-Wege-Authentifizierung konfigurieren können.
Einstellungen für die Datenübertragung	Wenn Sie auf die Schaltfläche **Konfigurieren** klicken, wird ein Fenster geöffnet, in dem Sie die Einstellungen für die Datenübertragung an KATA-Server konfigurieren können.

Fenster "KATA-Server"

Dieses Fenster zeigt in Tabellenform eine Liste mit Einstellungen für die Verbindung zu den KATA-Servern an. Für jeden Server, zu dem eine Verbindung konfiguriert ist, listet die Tabelle die IP-Adresse (IPv4 oder IPv6) oder den vollqualifizierten Domänennamen (FQDN) und den Port des Servers auf.

Mit den Schaltflächen und dem Menü über der Tabelle können Sie Folgendes tun:

- Verbindungseinstellungen zu einem KATA-Server hinzufügen.
- Bereits konfigurierte Verbindungseinstellungen ändern oder löschen.
- Eine Liste mit den konfigurierten Verbindungseinstellungen exportieren oder importieren.

Fenster zum Hinzufügen von Parametern für die Verbindung mit dem KATA-Server

In diesem Fenster können Sie die Parameter für die Verbindung zum KATA-Server festlegen.

Einstellungen der Verbindung mit dem KATA-Server

Einstellung	Beschreibung
Adresse	Adresse des KATA-Servers. Sie können die IP-Adresse (IPv4 oder IPv6) oder den vollqualifizierten Domänennamen (FQDN) des Servers angeben. Um sicherzustellen, dass die Kommunikation mit dem KATA-Server nicht unterbrochen wird, wenn die App bei aktivierter Netzwerkisolation des Geräts ausfällt, wird es empfohlen, die IP-Adresse des Servers anzugeben. Der Standardwert ist `127.0.0.1`.
Port	Port für die Verbindung zum KATA-Server. Der Standardwert ist `443`.

Fenster zum Konfigurieren der Verbindungseinstellungen mit den Servern

In diesem Fenster können Sie die allgemeinen Verbindungseinstellungen mit den KATA-Servern konfigurieren.

Einstellungen für die Verbindung mit den KATA-Servern

Einstellung	Beschreibung
Synchronisationsanfrage an den KATA-Server senden alle (Min.)	Häufigkeit des Sendens von Synchronisierungsanfragen an den KATA-Server in Minuten. Standardwert: 5.
Maximale Wartezeit für den Verbindungsaufbau mit einem Server (Sek.)	Die maximale Wartezeit auf eine Verbindung mit dem KATA-Server in Sekunden. Der Standardwert ist `10`.
Maximale Wartezeit für eine Serverantwort (Sek.)	Die maximale Wartezeit auf eine Antwort vom KATA-Server in Sekunden. Der Standardwert ist `10`.
Übertragung von Telemetriedaten erlauben	Aktiviert und deaktiviert des Sendens von Daten über Ereignisse auf Geräten (Telemetriedaten) an den KATA-Server. Standardmäßig ist das Senden von Telemetriedaten aktiviert.
Zwei-Wege-Authentifizierung verwenden	Aktiviert oder deaktiviert die Verwendung der Zwei-Wege-Authentifizierung für eine zusätzliche Absicherung der Verbindung zum KATA-Server. Um die bidirektionale Authentifizierung zu verwenden, müssen Sie ein Client-Zertifikat hinzufügen. Auf der Seite des KATA-Servers muss die bidirektionale Authentifizierung aktiviert sein.

Hinzufügen (des Client-Zertifikats)	Öffnet ein Fenster zum Hinzufügen eines Client-Zertifikats, um die Verbindung mit dem KATA-Server zusätzlich abzusichern. Die Schaltfläche wird angezeigt, wenn noch kein Client-Zertifikat hinzugefügt wurde. Wenn Sie die Verbindung zusätzlich absichern möchten, müssen Sie der Seite des KATA-Servers die Überprüfung des Client-Zertifikats aktivieren und in diesem Fenster das Kontrollkästchen **Zwei-Wege-Authentifizierung verwenden** aktivieren.
Löschen (des Client-Zertifikats)	Löscht das Client-Zertifikat. Die Schaltfläche wird angezeigt, wenn ein Client-Zertifikat hinzugefügt wurde.
Hinzufügen (des Serverzertifikats)	Öffnet ein Fenster zum Hinzufügen eines Serverzertifikats. Die Schaltfläche wird angezeigt, wenn noch kein Serverzertifikat hinzugefügt wurde.
Löschen (des Serverzertifikats)	Löscht das Serverzertifikat. Diese Schaltfläche wird angezeigt, wenn ein Serverzertifikat hinzugefügt wurde.

Fenster zum Hinzufügen eines Serverzertifikats

In diesem Fenster können Sie das Zertifikat eines KATA-Servers auf eine der folgenden Arten hinzufügen:

- Geben Sie den Pfad zur Zertifikatsdatei im Feld **Aus Datei hinzufügen** an. Mit der Schaltfläche **Durchsuchen** wird ein Standardfenster für die Dateiauswahl geöffnet. Geben Sie den Pfad zu einer Zertifikatsdatei im der- oder pem-Format an.
- Inhalt der Zertifikatsdatei in das Feld **Zertifikatdetails angeben** kopieren.

Wenn ein Serverzertifikat hinzugefügt wird, überprüft Kaspersky Endpoint Security das Serverzertifikat, um die Sicherheitsstufe der Verbindung zu erhöhen.

Fenster zum Hinzufügen eines Client-Zertifikats

In diesem Fenster können Sie für zusätzlichen Schutz der Verbindung mit KATA-Server ein Client-Zertifikat hinzufügen.

Wenn Sie die Verbindung zusätzlich absichern möchten, müssen Sie der Seite des KATA-Servers die Überprüfung des Client-Zertifikats aktivieren und im Fenster zum Konfigurieren der Verbindungseinstellungen mit dem Server das Kontrollkästchen **Zwei-Wege-Authentifizierung verwenden**.

Um ein Client-Zertifikat hinzuzufügen, geben Sie den Pfad zu dem Crypto-Container (Archiv im pfx-Format) an, der das Client-Zertifikat und den privaten Schlüssel enthält. Mit der Schaltfläche **Durchsuchen** wird ein Standardfenster für die Dateiauswahl geöffnet. Wenn das Archiv durch ein Kennwort geschützt ist, geben Sie das Kennwort in das Feld **Kennwort des Crypto-Containers** ein.

Fenster "Einstellungen der Datenübertragung"

In diesem Fenster können Sie die Einstellungen für die Datenübertragung an die KATA-Server konfigurieren.

Einstellungen zur Datenübertragung an die KATA-Server

Einstellung	Beschreibung
Maximale Verzögerung beim Versenden von Ereignissen (Sek.)	Maximale Verzögerung beim Senden von Ereignissen an den KATA-Server in Sekunden. Der Standardwert ist `30`.
Begrenzung für die Anzahl an Ereignissen aktivieren	Aktiviert oder deaktiviert die Beschränkung der Anzahl an Ereignissen, die an den KATA-Server gesendet werden.
Maximale Anzahl an Ereignissen pro Stunde	Die maximale Anzahl an Ereignissen innerhalb einer Stunde. Der Standardwert ist `3000`.
Maximale Anzahl an Ereignissen eines Typs in Prozent	Maximale Anzahl an Ereignissen eines Typs in Prozent. Die Übertragung von Ereignissen wird begrenzt, wenn das Verhältnis von Ereignissen des gleichen Typs (z. B. Änderung der Registrierung) zur Gesamtzahl der Ereignisse die prozentuale Grenze überschreitet. Der Standardwert ist `15`.

Integration mit Kaspersky Endpoint Detection and Response (KATA) über die Befehlszeile einrichten

Über die Befehlszeile können Sie die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response (KATA) mithilfe der vordefinierten Aufgabe "Integration mit Kaspersky Endpoint Detection and Response (KATA)" (*KATAEDR*) verwalten.

Standardmäßig wird die Aufgabe "Integration mit Kaspersky Endpoint Detection and Response (KATA)" nicht gestartet. Sie können diese Aufgabe manuell starten und beenden.

Sie können Einstellungen für die Integration mit Kaspersky Endpoint Detection and Response (KATA) konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe ändern.

Mithilfe von Befehlen zur Verwaltung der Einstellungen für die Integration mit Kaspersky Endpoint Detection and Response (KATA) können Sie Zertifikate verwalten, die für die Verbindung zu den KATA-Servern verwendet werden.

Einstellungen der Aufgabe zur Kaspersky Endpoint Detection and Response (KATA)

Die folgende Tabelle beschreibt alle verfügbaren Einstellungen und Standardwerte für alle Einstellungen, die Sie für die Aufgabe zur Integration mit Kaspersky Endpoint Detection and Response (KATA) festlegen können.

Einstellungen der Aufgabe zur Kaspersky Endpoint Detection and Response (KATA)

Einstellung	Beschreibung	Wert
`Address`	Adresse des KATA-Servers. Sie können die IP-Adresse (IPv4 oder IPv6) oder den vollqualifizierten Domänennamen (FQDN) des Servers angeben. Um sicherzustellen, dass die Kommunikation mit dem KATA-Server nicht unterbrochen wird, wenn die App bei aktivierter Netzwerkisolation des Geräts ausfällt, wird es empfohlen, die IP-Adresse des Servers anzugeben.	Der Standardwert ist `127.0.0.1`.
`Port`	Port für die Verbindung zum KATA-Server.	Der Standardwert ist `443`.
`UseClientPinnedCertificate`	Aktivieren und Deaktivieren der Zwei-Wege-Authentifizierung, um die Verbindung zum KATA-Server zusätzlich abzusichern. Wenn die Zwei-Wege-Authentifizierung auf der Seite des KATA-Servers aktiviert ist, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen der Aufgabe zur Integration mit Kaspersky Endpoint Detection and Response (KATA) aktivieren und ein Client-Zertifikat hinzufügen, bevor Sie die Aufgabe ausführen.	`Yes` – die Zwei-Wege-Authentifizierung wird zum zusätzlichen Absichern der Verbindung zum KATA-Server verwendet `No` (Standardwert) – die Zwei-Wege-Authentifizierung wird nicht verwendet
`SynchronizationPeriod`	Häufigkeit des Sendens von Synchronisierungsanfragen an den KATA-Server in Minuten.	Der Standardwert ist `5`.
`ConnectionTimeout`	Die maximale Wartezeit auf eine Verbindung mit dem KATA-Server in Sekunden.	Der Standardwert ist `10`.
`RequestTimeout`	Die maximale Wartezeit auf eine Antwort vom KATA-Server in Sekunden.	Der Standardwert ist `10`.
`MaximumDataTransferTime`	Maximale Verzögerung beim Senden von Ereignissen an den KATA-Server in Sekunden.	Der Standardwert ist `30`.
`UseRequestCountLimits`	Aktivieren und Deaktivieren der Begrenzung der Anzahl der an den KATA-Server gesendeten Ereignisse.	`Yes` (Standardwert) – die Anzahl der gesendeten Ereignisse wird begrenzt `No` – die Anzahl der gesendeten Ereignisse wird nicht begrenzt
`MaximumNumberOfEventsInHour`	Die maximale Anzahl an Ereignissen innerhalb einer Stunde.	Der Standardwert ist

		`3000`.
`EventLimitExceededPercentage`	Maximale Anzahl an Ereignissen eines Typs in Prozent. Die Übertragung von Ereignissen wird begrenzt, wenn das Verhältnis von Ereignissen des gleichen Typs zur Gesamtzahl der Ereignisse die prozentuale Grenze überschreitet.	Der Standardwert ist `15`.
`EnableTelemetry`	Aktivieren und Deaktivieren des Sendens von Daten über Ereignisse auf Geräten (Telemetriedaten) an den KATA-Server.	`Ja` (Standardwert) – Telemetriedaten an den KATA-Server senden `Nein` – keine Telemetrie senden

Verwaltung der Zertifikate für die Verbindung mit KATA-Servern

Für das Verwalten der Zertifikate sind Root-Berechtigungen erforderlich.

Sie können die Zertifikate, die für die Verbindung zu KATA-Servern verwendet werden, mithilfe von Befehlen verwalten. Mit Zertifikaten können Sie folgende Vorgänge ausführen:

- Hinzufügen oder Ersetzen des Serverzertifikats
- Anzeigen von Informationen zum Serverzertifikat
- Löschen des Serverzertifikats
- Hinzufügen oder Ersetzen des Client-Zertifikats
- Anzeigen von Informationen zum Client-Zertifikat
- Löschen des Client-Zertifikats

Um ein Serverzertifikat hinzuzufügen oder zu ersetzen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --add-kataedr-server-certificate <Dateiname und Dateipfad>
```

wobei `< Dateiname und Dateipfad >` dem Namen und Pfad der Datei entsprechen, die das Serverzertifikat enthält.

Um ein Client-Zertifikat hinzuzufügen oder zu ersetzen:

1. Führen Sie den Befehl aus:

   ```
   kesl-control [-R] --add-kataedr-client-certificate <Dateiname und Dateipfad>
   ```

   wobei `< Dateiname und Dateipfad >` dem Namen und Pfad des Crypto-Containers (Archiv im pfx-Format) entsprechen, der den geheimen Schlüssel enthält.

2. Wenn der Crypto-Container durch ein Kennwort geschützt ist, geben Sie das Kennwort ein, wenn Sie dazu aufgefordert werden.

Das Client-Zertifikat wird verwendet, um die Verbindung zum KATA-Server zusätzlich abzusichern, wenn die Überprüfung des Client-Zertifikats in den Einstellungen des KATA-Servers aktiviert ist und der Parameter "UseClientPinnedCertificate" in den Einstellungen der Aufgabe zur Integration mit Kaspersky Endpoint Detection and Response (KATA) auf yes gestellt ist.

Um Informationen zum Zertifikat anzuzeigen, führen Sie den folgenden Befehl aus:

- Für ein Serverzertifikat:

  ```
  kesl-control [-R] --query-kataedr-server-certificate
  ```

- Für ein Client-Zertifikat:

  ```
  kesl-control [-R] --query-kataedr-client-certificate
  ```

  Als Ausführungsergebnis des Befehls werden die folgenden Informationen zum Zertifikat angezeigt:

- Seriennummer des Zertifikats
- Zertifikatinhaber
- Zertifikataussteller
- Beginn der Gültigkeitsdauer des Zertifikats
- Ende der Gültigkeitsdauer des Zertifikats
- SHA1- und SHA256-Fingerabdrücke des Zertifikats

Um das Serverzertifikat zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --remove-kataedr-server-certificate
```

Um das Client-Zertifikat zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --remove-kataedr-client-certificate
```

Wenn die Verwendung eines Zertifikats in den Einstellungen der Aufgabe zur Integration mit Kaspersky Endpoint Detection and Response (KATA) konfiguriert ist und die Aufgabe ausgeführt wird, schlägt das Löschen dieses Zertifikats fehl.

Integration mit Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum ist eine Lösung zum Schutz der IT-Infrastruktur eines Unternehmens vor Bedrohungen wie Exploits, Ransomware, dateilosen Angriffen (fileless attacks) und dem bösartigen Ausnutzen legitimer System-Tools zur Beschädigung von Geräten und Daten.

Kaspersky Endpoint Detection and Response Optimum überwacht und analysiert die Entwicklung einer Bedrohung und stellt zusätzlich dem Security Officer oder Administrator Informationen über einen potenziellen Angriff zur Verfügung, die für ein rechtzeitiges Ergreifen von Gegenmaßnahmen notwendig sind.

Die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Optimum erfolgt durch Kaspersky Endpoint Security – Endpoint Detection and Response Optimum (im Weiteren auch "EDR Optimum").

Kaspersky Endpoint Security 12.1 für Linux ist mit Kaspersky Endpoint Detection and Response Optimum Version 3.0 kompatibel.

In Kaspersky Endpoint Security für Linux bis Version 12.1 ist EDR Optimum nicht enthalten.

Kaspersky Endpoint Detection and Response Optimum verwendet die folgenden Tools zur Bedrohungsanalyse (Threat Intelligence):

- Die Infrastruktur des Cloud-Dienstes Kaspersky Security Network (im Folgenden auch KSN), welcher Zugriff auf die Wissensdatenbank von Kaspersky mit Reputation von Dateien, Websites und Software bietet.
- Die Integration mit dem Portal Kaspersky Threat Intelligence Portal, welches Informationen über die Reputation von Dateien und Websites enthält und anzeigt.
- Die Bedrohungsdatenbank Kaspersky Threats von Kaspersky.

Im Rahmen der Interaktion mit Kaspersky Endpoint Detection and Response Optimum kann Kaspersky Endpoint Security die folgenden Funktionen ausführen:

- Informationen über Ereignisse, die auf den Geräten stattfinden, an Kaspersky Security Center übermitteln. Kaspersky Endpoint Security sendet an Kaspersky Endpoint Security neben Überwachungsdaten zu Prozessen, offenen Netzwerkverbindungen und geänderten Dateien auch Daten zu den von der App erkannten Bedrohungen und zu den Verarbeitungsergebnissen dieser Bedrohungen an den KATA-Server.
- Ausführen von Reaktionsmaßnahmen, um die Sicherheitsfunktionen mittels der Befehle sicherzustellen, die von Kaspersky Security Center übertragen wurden.

Die Integration mit Kaspersky Endpoint Detection and Response Optimum besteht aus den folgenden Schritten:

1. **Aktivieren der erforderlichen Komponenten von Kaspersky Endpoint Security**

   Stellen Sie sicher, dass die folgenden Komponenten von Kaspersky Endpoint Security aktiviert sind und funktionieren:

   - Schutz vor bedrohlichen Dateien.
   - Schutz vor Web-Bedrohungen.
   - Verhaltensanalyse.

2. **Aktivieren der Tools zur Bedrohungsanalyse**

   Stellen Sie sicher, dass Kaspersky Security Network im Standard-Modus oder im erweiterten Modus aktiviert ist.

   Für eine optimale Ausführung von Kaspersky Endpoint Detection and Response Optimum wird es empfohlen, Kaspersky Security Network im erweiterten Modus zu verwenden.

3. **Aktivieren von EDR Optimum**

   Stellen Sie sicher, dass eine der folgenden Bedingungen erfüllt ist:

- Sie verwenden Kaspersky Endpoint Security unter einer Lizenz, welche die Funktionalitäten von Kaspersky Endpoint Detection and Response Optimum abdeckt.
- Sie haben eine separate Lizenz zur Nutzung der Funktionalitäten von Kaspersky Endpoint Detection and Response Optimum erworben und der App einen zusätzlichen Lizenzschlüssel für EDR Optimum hinzugefügt .

4 **Aktivieren der Integration mit Kaspersky Endpoint Detection and Response Optimum**

Standardmäßig ist die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Optimum deaktiviert. Sie können die Integration sowohl aktivieren und deaktivieren als auch deren Einstellungen konfigurieren:

- über die Web Console oder die Kaspersky Security Center Cloud Console
- Über die Befehlszeile

> Die Verwaltung von EDR Optimum über die Verwaltungskonsole von Kaspersky Security Center wird nicht unterstützt.

Sie können den Ausführungsstatus von EDR Optimum wie folgt überprüfen:

- Mittels des *Berichts über den Status der Anwendungskomponenten* in der Web Console oder der Kaspersky Security Center Cloud Console.

  Die Komponente **Endpoint Detection and Response Optimum** wurde zur Liste der Komponenten von Kaspersky Endpoint Security hinzugefügt. Weitere Informationen zum Umgang mit Berichten finden Sie in der Hilfe zu Kaspersky Security Center.
- In den Geräteeigenschaften in der Web Console oder der Kaspersky Security Center Cloud Console.
- Über die Befehlszeile.

5 **Aktivieren der Übertragung von Daten zum Administrationsserver**

Um alle Funktionen von Kaspersky Endpoint Detection and Response Optimum zu verwenden, müssen Sie die folgenden Einstellungen aktivieren:

- **Über Dateien im Backup-Speicher informieren aktiviert/deaktiviert**.

  Sie können diese Einstellung in den Richtlinieneigenschaften unter **App-Einstellungen** → **Allgemeine Einstellungen** → **Speichereinstellungen** aktivieren.

  Durch das Aktivieren dieser Einstellung gewähren Sie die Übertragung von Informationen über Dateien, die auf dem Gerät von Kaspersky Endpoint Security in das Backup verschoben wurden, an Kaspersky Security Center.
- **EDR-Alarme anzeigen**.

  Sie können diese Einstellung im Hauptfenster der Web Console im Abschnitt **Einstellungen** → **Einstellungen der Benutzeroberfläche** aktivieren.

  Wenn Sie die Einstellungen aktivieren, wird die Alarm-Liste angezeigt.

> In der Web Console bis Version 15.1 ist die Option **EDR-Alarme anzeigen** nicht verfügbar.

Integration mit Kaspersky Endpoint Detection and Response Optimum aktivieren und deaktivieren

Sie können die Integration mit Kaspersky Endpoint Detection and Response Optimum aktivieren oder deaktivieren:

- über die Web Console oder die Kaspersky Security Center Cloud Console
- Über die Befehlszeile

Das Verwalten der Einstellungen für die Integration mit Kaspersky Endpoint Detection and Response Optimum über die Verwaltungskonsole wird nicht unterstützt.

Integration mit Kaspersky Endpoint Detection and Response Optimum in der Web Console aktivieren und deaktivieren

In der Web Console oder der Kaspersky Security Center Cloud Console können Sie die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Optimum aktivieren oder deaktivieren und die Integrationseinstellungen auf folgende Arten konfigurieren:

- In den Richtlinieneigenschaften (**App-Einstellungen** → **Detection and Response** → **Endpoint Detection and Response Optimum**)
- In den Geräteeigenschaften (**Assets (Geräte)** → **Verwaltete Geräte**) → Link <Gerätename> → **Anwendung** → Link <Name von Endpoint Security 12.1 für Linux> → **App-Einstellungen** → **Detection and Response** → **Endpoint Detection and Response Optimum**).

  Das Aktivieren oder Deaktivieren der Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Optimum ist in den Geräteeigenschaften nicht verfügbar, wenn das Gerät durch eine Richtlinie abgedeckt ist.

Integrationseinstellungen mit Kaspersky Endpoint Detection and Response Optimum

Einstellung	Beschreibung
Endpoint Detection and Response Optimum ist aktiviert/deaktiviert	Aktiviert oder Deaktiviert die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Optimum. Die Integration ist standardmäßig deaktiviert.
Netzwerkisolation	Über den Link **Einrichten der Gerätefreigabe**, wird das Fenster **Einrichten der Gerätefreigabe** geöffnet, in dem Sie die Dauer der Geräteblockierung konfigurieren können.
Ausschlüsse	Der Link **Ausnahmen** öffnet das Fenster Ausnahmen, in dem Sie die Ausnahmen für die Netzwerkisolation konfigurieren können.

Integration mit Kaspersky Endpoint Detection and Response Optimum über die Befehlszeile aktivieren und deaktivieren

Über die Befehlszeile können Sie die Integration mit Kaspersky Endpoint Detection and Response Optimum mithilfe des Parameters `UseEdrOptimum` in den allgemeinen App-Einstellungen aktivieren oder deaktivieren.

Sie können den Wert des Parameters mithilfe von Befehlszeilenschaltern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen App-Einstellungen enthält.

Um die Integration mit Kaspersky Endpoint Detection and Response Optimum über den Befehlszeilenparameter zu aktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

Um die Integration mit Kaspersky Endpoint Detection and Response Optimum über den Befehlszeilenparameter zu deaktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings UseEdrOptimum=No
```

Status der Integration mit Kaspersky Endpoint Detection and Response anzeigen (KATA)

Status der Integration in der Web Console oder der Kaspersky Security Center Cloud Console anzeigen

Sie können den Status der Integration mit Kaspersky Endpoint Detection and Response Optimum in der Web Console oder der Kaspersky Security Center Cloud Console auf folgende Weise anzeigen: Wechseln Sie zum Abschnitt **Assets (Geräte)** → **Verwaltete Geräte** → Link <Gerätename> → **Anwendungen** → <Name von Kaspersky Endpoint Security 12.1 für Linux> → **Allgemein** → **Komponenten**.

Status der Integration über die Befehlszeile anzeigen

Sie können den Status der Integration mit Kaspersky Endpoint Detection and Response Optimum über die Befehlszeile anzeigen, indem Sie den Befehl `kesl-control --app-info` ausführen.

Statuswerte für die Integration

Für EDR Optimum wird einer der folgenden Statuswerte angezeigt:

- *Wird ausgeführt*.

  Dieser Status wird angezeigt, wenn die folgenden Bedingungen gleichzeitig erfüllt sind:

  - Es wurde ein Lizenzschlüssel hinzugefügt, der zur Ausführung von EDR Optimum erforderlich ist
  - Das aktuelle Datum überschreitet nicht das Ablaufdatum der Lizenz

- Es ist mindestens eine der Komponenten von Kaspersky Endpoint Security aktiviert, die für die Funktion von EDR Optimum erforderlich sind
- Die Integration mit Kaspersky Endpoint Detection and Response Optimum ist auf dem Gerät aktiviert

- *Angehalten*.

  Dieser Status wird in folgenden Fällen angezeigt:

  - Die Integration mit Kaspersky Endpoint Detection and Response Optimum ist deaktiviert
  - Kaspersky Endpoint Security wurde angehalten

- *Von der Lizenz nicht unterstützt*.

  Dieser Status wird in folgenden Fällen angezeigt:

  - Das aktuelle Datum überschreitet das Ablaufdatum der Lizenz
  - Die aktuelle Lizenz beinhaltet keine Funktionalität für EDR Optimum

- *Fehler*.

  Dieser Status wird angezeigt, wenn die folgenden Bedingungen gleichzeitig erfüllt sind:

  - Das aktuelle Datum überschreitet nicht das Ablaufdatum der Lizenz
  - Beim Ausführen mindestens einer der Komponenten von Kaspersky Endpoint Security, die für den Betrieb von EDR Optimum erforderlich sind, ist ein Fehler aufgetreten

Informationen zur erkannten Bedrohung und möglichen Reaktionsmaßnahmen anzeigen

Um alle Informationen zu einer erkannten Bedrohung anzuzeigen und Maßnahmen zur Reaktion auf diese Bedrohung durchzuführen, können Sie das Fenster mit den Alarmdetails verwenden. Das Fenster enthält folgende Informationen und Möglichkeiten:

- Diagramm mit der Entwicklungskette der Bedrohung
- Empfehlungen zur Reaktion auf eine Bedrohung mit der Möglichkeit, die ausgewählte Aktion auszuführen
- Allgemeine Informationen zur Erkennung einer Bedrohung (z. B. den Modus der Erkennung)
- Informationen über das geschützte Gerät
- Informationen über das erkannte Objekt
- Verlauf des Auftretens von Dateien auf dem Gerät
- Informationen über die Aktionen, die von der App ergriffen hat, um auf die erkannte Bedrohung zu reagieren

Weitere Informationen zum Arbeiten mit Alarmdetails finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum.

Die Aufbewahrungsdauer der Ergebnisse der IoC-Untersuchung beträgt 30 Tage. Danach beginnt Kaspersky Endpoint Security automatisch mit der Löschung alter Einträge.

Suche nach Kompromittierungsindikatoren

Mit der Aufgabe Suche nach Kompromittierungsindikatoren können Sie auf dem Gerät nach Anzeichen einer Kompromittierung suchen und mithilfe der Aufgabe *IOC-Untersuchung* Maßnahmen ergreifen, um auf eine Bedrohung zu reagieren.

Um nach Anzeichen einer Kompromittierung zu suchen, verwendet Kaspersky Endpoint Security IOC-Dateien, die vom Benutzer erstellt werden müssen. Die IOC-Dateien müssen den Anforderungen an IOC-Dateien entsprechen.

Sie können die Aufgabe IOC-Untersuchung erstellen, *ausführen* und deren Parameter in der Web Console oder der Kaspersky Security Center Cloud Console ändern:

- Über den Abschnitt **Assets (Geräte)** → **Aufgaben**
- Über den Abschnitt **Assets (geräte)** → **Verwaltete Geräte** → Link <Name des Geräts> → **Aufgaben**
- Im Fenster mit den Alarmdetails

Sie können eine Aufgabe zur *IOC-Untersuchung* nicht über die Befehlszeile erstellen, ausführen oder konfigurieren. Das Anzeigen der über die Web Console oder die Kaspersky Security Center Cloud Console erstellten Aufgabe *IoC-Untersuchung* ist in der Befehlszeile mit dem Befehl `kesl-control --get-task-list` nicht möglich.

Für diese Aufgabe ist in den Einstellungen des Zeitplans die Wake-on-LAN-Option nicht verfügbar. Um die Aufgabe auszuführen, stellen Sie sicher, dass das Gerät eingeschaltet ist.

Einstellungen der Aufgabe *IoC-Untersuchung*

Einstellung	Beschreibung
IOC-Dateien neu definieren	Über diese Schaltfläche wird der Bereich **IOC-Dateien neu definieren** geöffnet. Die im im Bereich **IOC-Dateien neu definieren** befindliche Schaltfläche **IOC-Dateien hinzufügen** öffnet ein Fenster, in dem Sie die für die Suche nach Kompromittierungsindikatoren erforderlich IOC-Dateien auf dem Gerät auswählen und herunterladen können. Nach dem Herunterladen der IOC-Dateien können Sie die Liste der Indikatoren aus den IOC-Dateien anzeigen.
IOC-Sammlung exportieren	Über diese Schaltfläche werden die IOC-Dateien auf das Gerät heruntergeladen.
Anzuwendende Aktion als Reaktion auf ein erkanntes IOC	Das Kontrollkästchen aktiviert oder deaktiviert die Anwendung von Antwort-Reaktionen auf erkannte Anzeichen einer Gefährdung. Wenn das Kontrollkästchen aktiviert ist und Anzeichen einer Gefährdung erkannt werden, führt die App die von Ihnen ausgewählten Reaktionen aus: • **Gerät vom Netzwerk isolieren**. Wenn dieses Kontrollkästchen aktiviert ist und Anzeichen einer Gefährdung erkannt werden, isoliert die App das Gerät vom Netzwerk, um eine Ausbreitung der Bedrohung zu verhindern. Sie können die Dauer der Isolation anpassen. • **Untersuchung wichtiger Bereiche starten**.

	Wenn das Kontrollkästchen aktiviert ist und Anzeichen einer Gefährdung erkannt werden, führt startet die App die Aufgabe *Untersuchung wichtiger Bereiche*. Standardmäßig überprüft Kaspersky Endpoint Security den Kernel-Speicher, die gestarteten Prozesse und die Bootsektoren. Wenn dieses Kontrollkästchen deaktiviert ist und Anzeichen einer Gefährdung erkannt werden, führt die App keine Antwort-Reaktionen aus. Informationen zur Erkennung von Kompromittierungsindikatoren werden sowohl im Fenster mit den Alarmdetails als auch in den Aufgabeneigenschaften angezeigt.
Untersuchungsbereiche	Es werden die Bereiche der Dateiuntersuchung angezeigt: wichtige Bereiche von Systemlaufwerken und der Pfad aus dem IOC.

Es wird nicht empfohlen, IOC-Dateien nach dem Start der Aufgabe hinzuzufügen oder zu entfernen. Dies kann zu einer fehlerhaften Anzeige von Ergebnissen der IOC-Untersuchung für frühere Aufgabenausführungen führen. Um eine Suche nach Kompromittierungsindikatoren mit neuen IOC-Dateien auszuführen, wird es empfohlen, eine neue Aufgabe hinzuzufügen.

Das Ausführungsergebnis der Aufgabe *IoC-Untersuchung* kann im Abschnitt **Assets (Geräte)** → **Aufgaben** → <Aufgabenname> → **App-Einstellungen** → **Ergebnisse der IoC-Untersuchung** angezeigt werden.

Die Tabelle im Abschnitt **Ergebnisse der IoC-Untersuchung** enthält eine Liste der Geräte, auf denen die Aufgabe *IoC-Untersuchung* ausgeführt wurde, sowie die Ausführungsergebnisse der Aufgabe. In der Dropdown-Liste **Gerät** können Sie die Ergebnisse der Aufgabenausführung für alle verwalteten Geräte in der Administrationsgruppe oder für ein bestimmtes Gerät auswählen.

Folgende Spalten sind in der Tabelle enthalten:

- **Status**.

  Als Symbol angezeigter Erkennungsstatus der Kompromittierungsindikatoren.

- **Gerät**.

  Der Name des Geräts, auf dem die Aufgabe *IoC-Untersuchung* ausgeführt wurde.

- **Uhrzeit**.

  Datum und Uhrzeit der Ausführung der Aufgabe *IoC-Untersuchung*.

- **Ergebnisse**.

  Informationen zum Ergebnis der Aufgabe *IoC-Untersuchung*. Als Ergebnis der Aufgabenausführung kann einer der folgenden Statuswerte angezeigt werden:

  - *IOCs erkannt*

    Dieser Status wird als Link angezeigt, der beim Anklicken ein Fenster mit den Alarmdetails öffnet.

  - *Keine IOCs erkannt*.

Zusätzlich kann das Resultat der Aufgabenausführung im Abschnitt **Assets (Geräte)** → **Aufgaben** → <Aufgabenname> auf der Registerkarte **Ergebnisse** in der Spalte **Beschreibung** angezeigt werden.

Die Aufbewahrungsdauer der Ergebnisse der IoC-Untersuchung beträgt 30 Tage. Danach beginnt Kaspersky Endpoint Security automatisch mit der Löschung alter Einträge.

Anforderungen an IOC-Dateien

Beim Erstellen von IOC-Suchaufgaben sind die folgenden Anforderungen und Einschränkungen in Bezug auf IOC-Dateien beachten:

- Die App unterstützt IOC-Dateien mit IOC- und XML-Erweiterungen, die dem offenen Standard zur Beschreibung von Kompromittierungsindikatoren OpenIOC 1.0 und 1.1 entsprechen.
- Semantische Fehler und von IOC nicht unterstützte Begriffe und Tags in den IOC-Dateien verursachen keine Fehler bei der Aufgabenausführung. Für solche Abschnitte in IOC-Dateien werden von der App fehlende Übereinstimmungen festgehalten.
- Die IDs aller IOC-Dateien, die innerhalb einer IOC-Suchaufgabe verwendet werden, müssen eindeutig sein. Das Vorhandensein von IOC-Dateien mit denselben IDs kann die Korrektheit der Ergebnisse der Aufgabenausführung beeinträchtigen.
- Die Größe einer IOC-Datei sollte 2 MB nicht überschreiten. Die Verwendung größerer Dateien führt dazu, dass Aufgaben zur IOC-Untersuchung fehlschlagen. Die Gesamtgröße aller zur IOC-Sammlung hinzugefügten Dateien sollten 10 MB nicht überschreiten. Die Gesamtgröße 10 MB überschreitet, müssen Sie die IOC-Sammlung aufteilen und mehrere Aufgaben zur *IoC-Untersuchung* erstellen.
- Es wird empfohlen, für jede Bedrohung eine IOC-Datei zu erstellen. Dadurch sind die Resultate der Aufgabe *IoC-Untersuchung* leichter ablesbar.

Über den unteren Link können Sie eine Datei herunterladen, die eine Tabelle mit einer vollständigen Liste der IOC-Begriffe des OpenIOC-Standards enthält.

IOC_TERMS.XLSX HERUNTERLADEN

In der folgenden Tabelle sind Besonderheiten und Einschränkungen der App bei der Unterstützung des OpenIOC-Standards aufgeführt.

Besonderheiten und Einschränkungen bei der Unterstützung des OpenIOC-Standards 1.0 und 1.1

Unterstützte Bedingungen	OpenIOC 1.0: • `is` • `isnot` (als Ausnahme aus einer Menge) • `contains` • `containsnot` (als Ausnahme aus einer Menge) OpenIOC 1.1: • `is` • `contains` • `starts-with` • `ends-with`

	• `matches` • `greater-than` • `less-than`
Unterstützte Attribute der Bedingungen	OpenIOC 1.1: • `preserve-case` • `negate`
Unterstützte Operatoren	`AND` `OR`
Unterstützte Datentypen	`"date"`: Datum (anwendbare Bedingungen: `is`, `greater-than`, `less-than`) `"int"`: Ganzzahl (anwendbare Bedingungen: `is`, `greater-than`, `less-than`) `"string"`: Zeichenkette (anwendbare Bedingungen: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: Dauer in Sekunden (anwendbare Bedingungen: `is`, `greater-than`, `less-than`)

Besonderheiten bei der Datentypinterpretation	Die Datentypen `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"` und `"base64Binary"` werden als Zeichenketten (string) interpretiert.
	Die App unterstützt die Interpretation des Parameters `Content` als Bereichsangabe für die Datentypen `int` und `date`:
	• OpenIOC 1.0:
	Unter Verwendung des Operators `TO` im Feld `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	• OpenIOC 1.1:
	• Unter Verwendung der Bedingungen `greater-than` und `less-than`
	• Unter Verwendung des Operators `TO` im Feld `Content`
	Die Anwendung unterstützt die Interpretation der Datentypen `date` und `duration`, wenn die Indikatoren im Format `ISO 8601, Zulu-Zeitzone und UTC` angegeben sind.

Netzwerkisolation eines Geräts aktivieren und deaktivieren

Sie können die Netzwerkisolation von Geräten mittels folgenden Methoden aktivieren:

- Mittels der Aufgabe zur *IoC-Untersuchung*.

  Wenn Sie beim Erstellen und Konfigurieren der Aufgabenparameter für die IoC-Untersuchung im Block **Aktionen bei Erkennung eines IOCs** die Kontrollkästchen **Anzuwendende Aktion als Reaktion auf ein erkanntes IOC** und **Gerät vom Netzwerk isolieren** aktivieren, wird die Netzwerkisolation automatisch aktiviert, sobald die App Kompromittierungsindikatoren (IOC) erkennt.

- Im Fenster mit den Alarmdetails
- In den Geräteeigenschaften in der Web Console oder der Kaspersky Security Center Cloud Console.

> Die Aktivierung der Netzwerkisolation ist nur verfügbar, wenn die Integration mit Kaspersky Endpoint Detection and Response Optimum-Lösung ist und die Komponente "EDR Optimum" den Status Wird ausgeführt besitzt.

Sie können die Netzwerkisolation von Geräten mittels folgenden Methoden deaktivieren:

- Manuell in den Geräteeigenschaften in der Web Console oder der Kaspersky Security Center Cloud Console.
- Manuell über die Befehlszeile.
- Im Fenster mit den Alarmdetails
- Durch Einstellen der automatischen Deaktivierung in den Geräteeigenschaften oder den Richtlinieneigenschaften.

> Die Deaktivierung der Netzwerkisolation in den Geräteeigenschaften und in der Befehlszeile ist unabhängig von Folgenden Bedingungen verfügbar: Aktivierung der Integration mit Kaspersky Endpoint Detection and Response Optimum, Aktivierung der Komponente "EDR Optimum" und Abdeckung des Geräts durch eine Richtlinie.

Sie können für Netzwerkverbindungen auch Ausnahmen konfigurieren, die nicht isoliert werden sollen, wenn die Netzwerkisolation aktiviert wird.

Den Status der Netzwerkisolation können Sie über die Befehlszeile überprüfen.

Sobald die Netzwerkisolation aktiviert ist, unterbricht die App auf dem Gerät sämtliche aktive TCP/IP-Netzwerkverbindungen und blockiert das Herstellen neuer TCP/IP-Verbindungen, mit folgenden Ausnahmen:

- Verbindungen, die in den Ausnahmen für die Netzwerkisolation angegeben sind
- Verbindungen, die durch die Dienste von Kaspersky Endpoint Security initiiert werden
- Verbindungen, die durch den Kaspersky Endpoint Security Administrationsagent initiiert werden
- Verbindungen mit SVMs und Integrationsserver, wenn die App im Light Agent-Modus verwendet wird.

Ein isoliertes Gerät bekommt von EDR Optimum automatisch das Tag **ISOLATED FROM NETWORK** zugewiesen. Nachdem deaktivieren der Netzwerkisolation wird dieses Tag automatisch entfernt.

Allgemeine Informationen zum Abrufen einer Liste isolierter Geräte mittels Tag finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum.

Netzwerkisolation eines Geräts manuell in der Web Console aktivieren und deaktivieren

So aktivieren oder deaktivieren Sie für ein Gerät die Netzwerkisolation:

1. Wählen Sie im Hauptfenster der der Web Console oder der Kaspersky Security Center Cloud Console **Assets (Geräte)** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** oberhalb der Liste der verwalteten Geräte und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

   In der Liste werden nur die verwalteten Geräte der ausgewählten Administrationsgruppe angezeigt.

3. Wählen Sie in der Liste das erforderliche Gerät und und klicken Sie auf dessen Namen.

4. Wechseln Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts zur Registerkarte **Apps**.

5. Klicken Sie in der Liste der auf dem Gerät installierten Anwendungen auf den Namen der App **Kaspersky Endpoint Security 12.1 für Linux**.

   Das Eigenschaftenfenster der App wird geöffnet.

6. Gehen Sie zur Registerkarte **App-Einstellungen** .

7. Gehen Sie zum Abschnitt **Detection and Response** → **Endpoint Detection and Response Optimum**.

8. Führen Sie im Block mit den Einstellungen für die **Netzwerkisolation** einen der folgenden Schritte aus:

   - Um die Netzwerkisolierung des Geräts zu aktivieren, klicken Sie auf die Schaltfläche **Gerät vom Netzwerk isolieren**

   - Um die Netzwerkisolation eines Geräts zu deaktivieren, klicken Sie auf die Schaltfläche **Isoliertes Gerät freigeben**

Wenn Sie die Netzwerkisolation für ein Gerät aktivieren, weist Kaspersky Endpoint Security dem Gerät das Tag **ISOLATED FROM NETWORK** zu. Wenn Sie die Netzwerkisolierung für ein Gerät deaktivieren, entfernt Kaspersky Endpoint Security dieses Tag vom Gerät.

Automatisches Aktivieren der Netzwerkisolation konfigurieren

Sie können die Netzwerkisolation so konfigurieren, dass sie nach Ablauf eines angegebenen Zeitraums automatisch deaktiviert wird. Dies können Sie hier tun:

- In den Geräteeigenschaften.

  Die Einstellung zum automatischen Deaktivieren der Netzwerkisolation in den Geräteeigenschaften ist nicht verfügbar, wenn das Gerät einer Richtlinie unterliegt.

- In den Richtlinieneigenschaften.

  Die in den Richtlinieneigenschaften angegebenen Einstellungen zum automatischen Deaktivieren der Netzwerkisolation gelten nur für Geräte, die aufgrund der Erkennung von Kompromittierungsindikatoren (Indicators of Compromise, IOC) während der Ausführung der Aufgabe *IoC-Untersuchung* isoliert wurden.

Standardmäßig deaktiviert die App die Netzwerkisolation 5 Stunden nachdem die aktiviert wurde. Nach dem Deaktivieren der Netzwerkisolation ist das Gerät uneingeschränkt im Netzwerk verfügbar.

Konfigurieren der automatischen Deaktivierung der Netzwerkisolation in den Geräteeigenschaften

So konfigurieren Sie für ein Gerät das automatische Deaktivieren der Netzwerkisolation:

1. Wählen Sie im Hauptfenster der der Web Console oder der Kaspersky Security Center Cloud Console **Assets (Geräte)** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** über der Liste der verwalteten Geräte und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

   In der Liste werden nur die verwalteten Geräte der ausgewählten Administrationsgruppe angezeigt.

3. Wählen Sie in der Liste das erforderliche Gerät und klicken Sie auf dessen Namen.

4. Wechseln Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts zur Registerkarte **Apps**.

5. Klicken Sie in der Liste der auf dem Gerät installierten Anwendungen auf den Namen der App **Kaspersky Endpoint Security 12.1 für Linux**.

   Das Eigenschaftenfenster der App wird geöffnet.

6. Gehen Sie zur Registerkarte **App-Einstellungen** .

7. Gehen Sie zum Abschnitt **Detection and Response** → **Endpoint Detection and Response Optimum**.

8. Klicken Sie im Block mit den Einstellungen der **Netzwerkisolation** auf den Link **Einrichten der Gerätefreigabe**.

9. Legen Sie im neuen Fenster **Einrichten der Gerätefreigabe** die Parameter für die Gerätefreigabe fest.

   Parameter für die Gerätefreigabe

Einstellung	Beschreibung
Automatisch isoliertes Gerät freigeben nach	Das Kontrollkästchen aktiviert oder deaktiviert die automatische Freigabe des isolierten Geräts nach der im Eingabefeld **Stunden** angegebenen Zeitspanne. Das Kontrollkästchen ist standardmäßig aktiviert.
Stunden	Eingabefeld für den Zeitraum in Stunden, nach dem das isolierte Gerät automatisch freigegeben wird. Dieses Feld ist nur aktiv, wenn das Kontrollkästchen **Automatisch isoliertes Gerät freigeben nach** aktiviert ist.

10. Speichern Sie Ihre Änderungen.

Konfigurieren der automatischen Deaktivierung der Netzwerkisolation in den Richtlinieneigenschaften

So konfigurieren Sie für ein Gerät das automatische Deaktivieren der Netzwerkisolation:

1. Wählen Sie im Hauptfenster der Web Console oder der Kaspersky Security Center Cloud Console die Option **Assets (Geräte)** → **Richtlinien und Richtlinienprofile**.

   Die Liste mit Richtlinien wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die die Geräte enthält, auf die die Richtlinie angewendet wird. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

   In der Liste werden die Richtlinien angezeigt, die für die ausgewählte Administrationsgruppe konfiguriert sind.

3. Klicken Sie in der Liste auf den Namen der erforderlichen Richtlinie.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.

4. Gehen Sie zur Registerkarte **App-Einstellungen** .

5. Gehen Sie zum Abschnitt **Detection and Response** → **Endpoint Detection and Response Optimum**.

6. Klicken Sie im Block mit den Einstellungen der **Netzwerkisolation** auf den Link **Einrichten der Gerätefreigabe**.

7. Legen Sie im neuen Fenster **Einrichten der Gerätefreigabe** die Parameter für die Gerätefreigabe fest.

   Parameter für die Gerätefreigabe

Einstellung	Beschreibung
Automatisch isoliertes Gerät freigeben nach	Das Kontrollkästchen aktiviert oder deaktiviert die automatische Freigabe des isolierten Geräts nach der im Eingabefeld **Stunden** angegebenen Zeitspanne. Das Kontrollkästchen ist standardmäßig aktiviert.
Stunden	Eingabefeld für den Zeitraum in Stunden, nach dem das isolierte Gerät automatisch freigegeben wird. Dieses Feld ist nur aktiv, wenn das Kontrollkästchen **Automatisch isoliertes Gerät freigeben nach** aktiviert ist.

8. Speichern Sie Ihre Änderungen.

Netzwerkisolation eines Geräts über die Befehlszeile deaktivieren

Um die Netzwerkisolation eines Geräts über die Befehlszeile zu deaktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --isolation-off
```

Den Status der Netzwerkisolation überprüfen und die Liste der Ausnahmen für die Netzwerkisolation anzeigen können Sie mit folgendem Befehl:

```
kesl-control [-R] --isolation-stat
```

Für die Netzwerkisolation zeigt die Befehlszeile einen der folgenden Statuswerte an:

- *Netzwerkisolation ist aktiviert.*
- *Netzwerkisolation ist deaktiviert.*

Ausnahmen für die Netzwerkisolation konfigurieren

Hier können Sie Ausnahmen konfigurieren:

- In den Richtlinieneigenschaften
- In den Geräteeigenschaften

Netzwerkverbindungen, die den angegebenen Regeln unterliegen, werden nach dem Aktivieren der Netzwerkisolation auf dem Gerät nicht blockiert.

Standardmäßig sind von der Netzwerkisolation jene Netzwerkprofile ausgeschlossen, die aus Regeln zur Sicherstellung eines unterbrechungsfreien Betriebs von Geräten mit DNS/DHCP-Server- und DNS/DHCP-Client-Rollen bestehen.

In den Richtlinieneigenschaften angegebene Ausnahmen werden nur angewendet, wenn die Netzwerkisolation von der App als Folge einer Reaktion auf die Erkennung eines Kompromittierungsindikators (IOC) automatisch aktiviert wird.

In den Geräteeigenschaften angegebene Ausnahmen werden nur angewendet, wenn die Netzwerkisolation in den Geräteeigenschaften oder im Fenster mit den Alarmdetails manuell aktiviert wird.

Eine aktive Richtlinie blockiert nicht die Anwendung von Ausnahmen für die Netzwerkisolation, die in den Geräteeigenschaften angegeben sind.

Hier können Sie eine Liste mit den Ausnahmen für die Netzwerkisolation anzeigen:

- In den Richtlinieneigenschaften (**App-Einstellungen** → **Detection and Response** → **Endpoint Detection and Response Optimum** → Link **Ausnahmen**)
- In den Geräteeigenschaften (**Assets (Geräte)** → **Verwaltete Geräte)** → Link <Gerätename> → Link <Name von Endpoint Security 12.1 für Linux> → **App-Einstellungen** → **Detection and Response** → **Endpoint Detection and Response Optimum** → Link **Ausnahmen**)
- Über die Befehlszeile

In der Web Console Ausnahmen für die Netzwerkisolation in den Richtlinieneigenschaften hinzufügen und entfernen

In der Web Console und der Kaspersky Security Center Cloud Console können Sie in den Richtlinieneigenschaften Ausnahmen für Netzwerkisolation hinzufügen und entfernen (Link **App-Einstellungen** → **Detection and Response** → **Endpoint Detection and Response Optimum** → **Ausnahmen**).

Im Fenster **Ausnahmen** können Sie mit den Schaltflächen oberhalb der Tabelle die folgenden Aktionen ausführen:

- Hinzufügen von Informationen über die ausgeschlossene Netzwerkverbindung mittels einer der folgenden Methoden:
  - Klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie anschließend die Informationen zur Netzwerkverbindung ein.
  - Klicken Sie auf die Schaltfläche **Aus Profil hinzufügen** und wählen Sie anschließend ein Netzwerkprofil aus der Liste aus.
- Löschen von Informationen über die Netzwerkverbindung

Ausnahmen für die Netzwerkisolation in den Geräteeigenschaften hinzufügen und entfernen

Das Hinzufügen oder Entfernen von Ausnahmen für die Netzwerkisolation ist in den Geräteeigenschaften nicht möglich, wenn das Gerät einer Richtlinie unterliegt.

So können Sie eine Ausnahme für die Netzwerkisolation hinzufügen oder entfernen:

1. Wählen Sie im Hauptfenster der Web Console die Option **Assets (Geräte)** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** über der Liste der verwalteten Geräte und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

   In der Liste werden nur die verwalteten Geräte der ausgewählten Administrationsgruppe angezeigt.

3. Wählen Sie in der Liste das erforderliche Gerät und klicken Sie auf dessen Namen.

4. Wechseln Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts zur Registerkarte **Apps**.

5. Klicken Sie in der Liste der auf dem Gerät installierten Anwendungen auf den Namen der App **Kaspersky Endpoint Security 12.1 für Linux**.

   Das Eigenschaftenfenster der App wird geöffnet.

6. Gehen Sie zur Registerkarte **App-Einstellungen** .

7. Gehen Sie zum Abschnitt **Detection and Response** → **Endpoint Detection and Response Optimum**.

8. Klicken Sie im Block mit den Parametern für die **Netzwerkisolation** auf den Link **Ausnahmen**, um das Fenster **Ausnahmen** zu öffnen.

9. Im neuen Fenster können Sie die Schaltflächen oberhalb der Tabelle benutzen, um die gewünschte Aktion auszuführen:

   - Wenn Sie Informationen zu einer ausgeschlossenen Netzwerkverbindung hinzufügen möchten, tun Sie dies mittels einer der folgenden Methoden:

     - Klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie Informationen zur Netzwerkverbindung ein.

     - Klicken Sie auf die Schaltfläche **Aus Profil hinzufügen** und wählen Sie ein Netzwerkprofil aus der Liste aus.

   - Wenn Sie Informationen zu einer auszuschließenden Netzwerkverbindung löschen möchten, aktivieren Sie das Kontrollkästchen neben der zu löschenden Netzwerkverbindung und klicken Sie auf die Schaltfläche **Löschen**.

10. Speichern Sie Ihre Änderungen.

Fenster "Ausnahme für die Netzwerkisolation hinzufügen"

In diesem Fenster können Sie Informationen über eine Netzwerkverbindung eingeben, die nach der Aktivierung der Netzwerkisolation nicht blockiert wird.

Einstellungen der Netzwerkverbindung

Einstellung	Beschreibung
Name	Name der Netzwerkverbindung
Richtung	Richtung der Netzwerkverbindung
Protokoll	Von der Netzwerkverbindung verwendetes Protokoll
Nummer	Nummer der Netzwerkverbindung
Lokale Ports/Portbereiche	Nummern der lokalen Ports/der Portbereiche
Remote-Ports/-Portbereiche	Nummern der Remote-Ports/der Bereiche der Remote-Ports
Remote-Adresse	IP-Adresse des Remote-Geräts

Fenster "Liste mit Netzwerkprofilen"

In diesem Fenster können Sie das Profil der auszuschließenden Netzwerkverbindung auswählen.

Profile der Netzwerkverbindungen

Profil der Netzwerkverbindung	Beschreibung
DNS-Server	Dienst der die Auflösung von DNS-Namen ermöglicht, indem er auf Anfragen zum Abrufen von IP-Adressen und zum Aktualisieren von DNS-Einträgen reagiert.
DNS-Client	Dienst der die Auflösung von DNS-Namen ermöglicht, indem er Abfragen von

	DNS-Namen durchführt.
Active Directory-Zertifikatdienste (AD CS)	Dienste zum Erstellen, Validieren und Widerrufen öffentlicher Schlüsselzertifikate für die interne Verwendung innerhalb einer Organisation.
Active Directory-Verbunddienste (AD FS)	Dienste zum Ermöglichen des Benutzerzugriffs auf mehrere Webdienste oder Netzwerkressourcen mithilfe eines einzigen zentral gespeicherten Satzes von Anmeldeinformationen.
Active Directory Lightweight Directory Services (AD LDS)	Dienste mit gleicher Funktionalität wie die Domänendienste von Active Directory, jedoch ohne Notwendigkeit der Erstellung von Domänen oder Domänencontrollern.
Active Directory Rights Management Services (AD RMS)	Dienste zur Steuerung des Benutzerzugriffs auf Dokumente.
DHCP	Dienst, der das Dynamic Host Configuration Protocol (DHCP) verwendet, um IP-Adressen automatisch zuzuweisen.
File Transfer Protocol (FTP)	Standard-Netzwerkprotokoll, das zum Übertragen von Dateien zwischen Clients und einem Server in einem Netzwerk verwendet wird.
Kerberos-Schlüsselverteilungscenter	Netzwerkdienst, der zur Bereitstellung von Tickets (TGS) und temporären Sitzungsschlüsseln für Benutzer und Geräte in einer Active Directory-Domäne verwendet wird.
Secure Shell (SSH)	Ein Protokoll, das die Remote-Verwaltung des Betriebssystems und das Tunneln von TCP-Verbindungen ermöglicht.
Linux-Systemkomponenten	Linux-Systemkomponenten.

Einen Prozess starten

Mit der Aufgabe *Prozess starten* können Sie erforderliche Prozesse und ausführbaren Dateien auf Geräten remote starten.

Beispielsweise können Sie:

- Prozesse starten, die aufgrund böswilliger Aktivitäten auf dem Gerät beendet wurden.
- Prozesse starten, die Sie beendet haben.

  Sie können beispielsweise einen Prozess, den Sie mit der Aufgabe *Prozess beenden* beendet haben, aus remote starten.
- Skripte.

  Sie können beispielsweise ein Skript ausführen, um Daten von einem Gerät zu sammeln, die zur Untersuchung einer Bedrohung gedacht sind.
- Tools.

  Sie können beispielsweise ein Tool ausführen, das die Informationen zu einer Gerätekonfiguration in einer Datei speichert.
- Anhänge.

Wenn auf Ihrem Betriebssystem SELinux im Modus `Enforcing` installiert ist, müssen Sie zum Ausführen der Aufgabe *Prozess starten* zusätzlich das SELinux-System konfigurieren.

Sie können die Aufgabe Prozess starten erstellen, *ausführen* und deren Parameter in der Web Console oder der Kaspersky Security Center Cloud Console ändern:

Sie können eine Aufgabe zur *Prozess starten* nicht über die Befehlszeile erstellen, ausführen oder konfigurieren. Das Anzeigen der über die Web Console oder die Kaspersky Security Center Cloud Console erstellten Aufgabe *Prozess starten* ist in der Befehlszeile mit dem Befehl `kesl-control --get-task-list` nicht möglich.

Parameter der Aufgabe zum Starten eines Prozesses

Einstellung	Beschreibung
Ausgeführter Befehl	Eingabefeld für den Startbefehl des Prozesses. Wenn Sie beispielsweise das Tool `klnagchk` ausführen möchten, mit dem die Verbindung zum Administrationsserver überprüft werden soll, müssen Sie den Befehl `/<Verzeichnisname>/klnagchk` eingeben und anschließend die übrigen in der unteren Tabelle beschriebenen Felder ausfüllen. Der Verzeichnisname kann auch im Feld **Pfad zum Arbeitsverzeichnis (optional)** eingegeben werden. In diesem Fall muss der Verzeichnisname nicht in das Feld **Auszuführender Befehl** eingegeben werden.
Befehlszeilenargumente (optional)	Eingabefeld für Befehlszeilenargumente zur Übergabe zusätzlicher Informationen an das Skript, das Tool oder die Anwendung beim Start. Sie können beispielsweise das Argument `-logfile klnagchk.log` eingeben. Dieses Argument teilt dem Tool mit, dass das Ergebnis der Ausführung in einer Datei mit dem Namen `klnagchk.log` gespeichert werden soll. Wenn Sie mehrere Argumente übergeben möchten, müssen Sie diese durch ein Leerzeichen trennen. Sie können beispielsweise die Argumente `-logfile klnagchk.log -savecert certificate.cer` eingeben. Diese Argumente teilen dem Tool mit, dass das Ergebnis der Ausführung in einer Datei mit dem Namen `klnagchk.log` gespeichert werden soll und dass das Zertifikat, das zur Überprüfung des Zugriffs auf den Administrationsserver verwendet wird, in der Datei `certificate.cer` gespeichert werden soll.
Pfad zum Arbeitsverzeichnis (optional)	Eingabefeld für den Pfad zum Arbeitsverzeichnis, in dem sich das Skript, das Tool oder die App zum Starten des Prozesses befindet. Sie können beispielsweise den Wert `/opt/kaspersky/klnagent64/bin/` eingeben. Wenn Sie im Feld **Auszuführender Befehl** einen Verzeichnisnamen eingegeben haben, muss das Feld **Pfad zum Arbeitsverzeichnis (optional)** nicht ausgefüllt werden.

Das Resultat der Aufgabenausführung kann im Abschnitt **Assets (Geräte)** → **Aufgaben** → <Aufgabenname> auf der Registerkarte **Ergebnisse** in der Spalte **Beschreibung** angezeigt werden.

Eines Prozesses beenden

Mit der Aufgabe *Prozess beenden* können Sie Prozesse auf einem Gerät aus remote beenden.

Beispielsweise können Sie:

- Prozesse beenden, die aufgrund böswilliger Aktivitäten auf dem Gerät gestartet wurden.
- Von Ihnen gestartete Prozesse beenden.

  Sie können beispielsweise einen Prozess, den Sie mit der Aufgabe *Prozess starten* gestartet haben, aus remote beenden.
- Skripte.

  Sie können beispielsweise ein Skript, dessen Ausführung Sie mit der Aufgabe *Prozess starten* gestartet haben, aus remote beenden.
- Tools.

  Sie können beispielsweise ein Tool zur Messung der Internet-Geschwindigkeitstest remote beenden, welches Sie vorher mit der Aufgabe *Prozess starten* gestartet haben.
- Anwendungen.

Das Beenden von Prozessen kritischer Systemobjekte (System Critical Object - SCO) ist nicht möglich. SCOs umfassen Dateien, die für die Ausführung des Betriebssystems und von Kaspersky Endpoint Security erforderlich sind.

Sie können die Aufgabe Prozess beenden erstellen, *ausführen* und deren Parameter in der Web Console oder der Kaspersky Security Center Cloud Console ändern: Sie können eine Aufgabe zur *Process beenden* nicht über die Befehlszeile erstellen, ausführen oder konfigurieren. Das Anzeigen der über die Web Console oder die Kaspersky Security Center Cloud Console erstellten Aufgabe *Prozess beenden* ist in der Befehlszeile mit dem Befehl `kesl-control --get-task-list` nicht möglich.

Parameter der Aufgabe zum Beenden eines Prozesses

Einstellung	Beschreibung
Geben Sie die Datei an, deren Prozesse beendet werden soll	In der Dropdown-Liste können Sie die Methode zur Pfadangabe auswählen: • **Nach Pfad zum Verzeichnis und Prüfsumme**. • **Nach vollständigem Pfad** • **Nach PID** Der Wert **Nach PID** wird in der Dropdown-Liste nur für Aufgaben angezeigt, die in den Geräteeigenschaften erstellt wurden.
Vollständiger Pfad zur Datei	Eingabefeld für den vollständigen Pfad zur Datei.

	Dieses Feld wird nur angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die Datei an, deren Prozesse beendet werden soll** die Option **Nach vollständigem Pfad** ausgewählt haben.
Typ der Prüfsumme	In der Dropdown-Liste können Sie die zu verwendende Prüfsumme der Datei auswählen: • **MD5**. • **SHA256**. Diese Dropdown-Liste wird nur angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die Datei an, deren Prozesse beendet werden soll** die Option **Nach Pfad zum Verzeichnis und Prüfsumme ausgewählt** haben.
Prüfsumme der Datei	Eingabefeld für die Prüfsumme der Datei Dieses Feld wird nur angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die Datei an, deren Prozesse beendet werden soll** die Option **Nach Pfad zum Verzeichnis und Prüfsumme** und in der Dropdown-Liste **Typ der Prüfsumme** den Wert **MD5** angegeben haben.
Pfad zum Verzeichnis	Eingabefeld für Pfad zum Dateiverzeichnis. Dieses Feld wird nur angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die Datei an, deren Prozesse beendet werden soll** die Option **Nach Pfad zum Verzeichnis und Prüfsumme** ausgewählt haben.
Prozess-ID	Eingabefeld für die Prozess-ID (PID) Dieses Feld wird nur angezeigt, wenn Sie in der Dropdown-Liste **Datei angeben, deren Prozesse beendet werden soll** die Option **Nach PID** ausgewählt haben.

Das Resultat der Aufgabenausführung kann im Abschnitt **Assets (Geräte)** → **Aufgaben** → <Aufgabenname> auf der Registerkarte **Ergebnisse** in der Spalte **Beschreibung** angezeigt werden.

Datei von Gerät abrufen

Mit der Aufgabe *Datei vom Gerät abrufen* können Sie Dateien von den Geräten der Benutzer abrufen.

Beispielsweise können Sie eine Ereignisprotokoll-Datei abrufen, die von der Anwendung eines Drittanbieters generiert wurde.

Sie können die Aufgabe Datei abrufen erstellen, *ausführen* und deren Parameter in der Web Console oder der Kaspersky Security Center Cloud Console ändern:

Sie können eine Aufgabe des Typs *Datei von Gerät abrufen* nicht über die Befehlszeile erstellen, ausführen oder konfigurieren. Das Anzeigen der über die Web Console oder die Kaspersky Security Center Cloud Console erstellten Aufgabe *Datei von Gerät abrufen* ist in der Befehlszeile mit dem Befehl `kesl-control --get-task-list` nicht möglich.

Die Tabelle **Datei abrufen** auf der Registerkarte **App-Einstellungen** enthält die folgenden Spalten:

- **Pfad zum Verzeichnis**.

  Pfad zum Verzeichnis der Datei, die sich auf dem Gerät befindet.

- **Prüfmethode der** Prüfsumme.

  Die Art der Berechnung der Prüfsumme der Datei, die sich auf dem Gerät befindet.

Mit den Schaltflächen oberhalb der Tabelle können Sie Daten zu Dateien, die sich auf dem Gerät befinden, hinzufügen, ändern oder löschen. Die Aufgabe *Datei von Gerät abrufen* wird für die Dateien ausgeführt, die in der Tabelle **Datei abrufen** angegebenen sind.

Wenn Sie auf die Schaltfläche **Hinzufügen** klicken, wird das Fenster **Datei abrufen** geöffnet, in dem Sie die Parameter der Aufgabe *Datei vom Gerät abrufen* konfigurieren können.

Parameter der Aufgabe zum Abrufen einer Datei von einem Gerät

Einstellung	Beschreibung
Geben Sie die abzurufende Datei an	In der Dropdown-Liste können Sie die Methode zur Pfadangabe auswählen: • **Nach Pfad zum Verzeichnis und Prüfsumme**. • **Nach vollständigem Pfad**
Vollständiger Pfad zur Datei	Eingabefeld für den vollständigen Pfad zur Datei. Dieses Feld wird nur angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die abzurufende Datei an** die Option **Nach vollständigem Pfad** ausgewählt haben.
Typ der Prüfsumme	In der Dropdown-Liste können Sie die zu verwendende Prüfsumme der Datei auswählen: • **MD5**. • **SHA256**. Diese Dropdown-Liste wird nur angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die abzurufende Datei an** die Option **Nach Pfad zum Verzeichnis und Prüfsumme** ausgewählt haben.
Prüfsumme der Datei	Eingabefeld für die Prüfsumme der Datei Dieses Feld wird nur angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die abzurufende Datei an** die Option **Nach Pfad zum Verzeichnis und Prüfsumme** ausgewählt haben.
Pfad zum	Eingabefeld für Pfad zum Dateiverzeichnis.

Verzeichnis der Datei	Dieses Feld wird nur angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die abzurufende Datei an** die Option **Nach Pfad zum Verzeichnis und Prüfsumme** ausgewählt haben.

Als Resultat der Ausführung der Aufgabe *Datei von Gerät abrufen* wird eine Kopie der Datei im Backup des Geräts gespeichert. Mittels der Web Console oder der Kaspersky Security Center Cloud Console können Sie die Kopie aus dem Backup auf das Gerät herunterladen, von dem aus Sie den Download initiiert haben.

Die Datei darf maximal 100 MB groß sein.

Die Originaldatei auf dem Gerät des Benutzers verbleibt im Originalverzeichnis.

Alle über die Aufgabe *Datei vom Gerät abrufen* empfangenen Dateien haben im Backup-Speicher von Kaspersky Security Center den Status *Infiziert*, unabhängig von den Ergebnissen der Dateiprüfung.

Das Resultat der Aufgabenausführung kann im Abschnitt **Assets (Geräte)** → **Aufgaben** → <Aufgabenname> auf der Registerkarte **Ergebnisse** in der Spalte **Beschreibung** angezeigt werden.

Datei von Gerät löschen

Sie können Dateien von einem Gerät löschen, indem Sie die Aufgabe *Datei von Gerät löschen* verwenden. Dies kann beispielsweise im Rahmen der Reaktion auf eine Bedrohungen erforderlich sein.

Kritische Systemobjekte (System Critical Objetc – SCO) können nicht gelöscht werden. SCOs umfassen Dateien, die für die Ausführung des Betriebssystems und von Kaspersky Endpoint Security erforderlich sind.

Sie können die Aufgabe Datei löschen erstellen, *ausführen* und deren Parameter in der Web Console oder der Kaspersky Security Center Cloud Console ändern:

Sie können eine Aufgabe des Typs *Datei von Gerät löschen* nicht über die Befehlszeile erstellen, ausführen oder konfigurieren. Das Anzeigen der über die Web Console oder die Kaspersky Security Center Cloud Console erstellten Aufgabe *Datei von Gerät löschen* ist in der Befehlszeile mit dem Befehl `kesl-control --get-task-list` nicht möglich.

Parameter der Aufgabe zum Löschen einer Datei von einem Gerät

Einstellung	Beschreibung
Geben Sie die zu löschende Datei an	In der Dropdown-Liste können Sie die Methode für die Pfadangabe zur zu löschenden Datei auswählen: • **Nach Pfad und Prüfsumme**. • **Nach vollständigem Pfad**
Vollständiger Pfad zur Datei	Eingabefeld für den vollständigen Pfad zur zu löschenden Datei.

	Dieses Feld wird nur angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die zu löschende Datei an** die Option **Nach vollständigem Pfad** ausgewählt haben.
Typ der Prüfsumme	In der Dropdown-Liste können Sie die zu verwendende Prüfsumme der zu löschenden Datei auswählen: • **MD5**. • **SHA256**. Dieses Dropdown-Liste wird nur angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die zu löschende Datei an** die Option **Nach Pfad und Prüfsumme** ausgewählt haben.
Prüfsumme der Datei	Eingabefeld für die Prüfsumme der zu löschenden Datei. Dieses Feld wird nur angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die zu löschende Datei an** die Option **Nach Pfad und Prüfsumme** ausgewählt haben.
Pfad zum Verzeichnis	Eingabefeld für Pfad zum Verzeichnis der zu löschenden Datei. Dieses Feld wird nur angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die zu löschende Datei an** die Option **Nach Pfad und Prüfsumme** ausgewählt haben.
Unterverzeichnisse einschließen	Dieses Kontrollkästchen schließt Unterverzeichnisse ein oder aus.

Wenn die Datei durch einem anderen Prozess gesperrt wird, wird die Aufgabe mit dem Status *Abgeschlossen* angezeigt, die Datei selbst wird jedoch erst nach einem Neustart des Geräts gelöscht. Stellen Sie nach einem Neustart des Geräts sicher, dass die Datei gelöscht wurde.

Die Aufgabe *Datei vom Gerät löschen* kann mit dem Fehler *Zugriff verweigert* abschließend, wenn Sie versuchen, eine laufende ausführbare Datei zu löschen. Erstellen Sie für diese Datei eine Aufgabe des Typs *Prozess beenden*, führen Sie diese aus und versuchen Sie es anschließend erneut.

Das Resultat der Aufgabenausführung kann im Abschnitt **Assets (Geräte)** → **Aufgaben** → <Aufgabenname> auf der Registerkarte **Ergebnisse** in der Spalte **Beschreibung** angezeigt werden.

Integration von Kaspersky Managed Detection and Response

Die Lösung "Kaspersky Managed Detection and Response" ermöglicht die kontinuierliche Suche, das Erkennen und das Eliminieren von Bedrohungen, die gegen Ihre Organisation gerichtet sind. Die Integration mit Kaspersky Managed Detection and Response erfolgt über Kaspersky Endpoint Security – Managed Detection and Response (im Weiteren auch "MDR").

Im Rahmen der Interaktion mit Kaspersky Managed Detection and Response kann Kaspersky Endpoint Security die folgenden Funktionen ausführen:

- Versand von Telemetriedaten an Kaspersky Managed Detection and Response zur Erkennung von Bedrohungen
- Ausführung der Befehle von Kaspersky Managed Detection and Response zur Bereitstellung der Schutzfunktionen

Um die Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response zu konfigurieren, gehen Sie wie folgt vor:

- Standardmäßig sind nur die Komponenten Schutz vor bedrohlichen Dateien und Verhaltensanalyse aktiviert. Wenn diese Komponenten deaktiviert sind, hat das Gerät in Kaspersky Managed Detection and Response einen roten Status.

  Es wird außerdem empfohlen, die Komponenten Schutz vor Web-Bedrohungen und Schutz vor Netzwerkbedrohungen zu aktivieren. Wenn diese Komponenten deaktiviert sind, hat das Gerät in Kaspersky Managed Detection and Response einen gelben Status.

  Nähere Informationen zu den Statuswerten finden Sie in der Hilfe zu Kaspersky Managed Detection and Response.

- Verwendung von Kaspersky Security Network im erweiterten Modus aktivieren.

  Sie können die Verwendung von Kaspersky Security Network über die Befehlszeile, in der Web Console oder in der Verwaltungskonsole aktivieren.

- Kaspersky Private Security Network konfigurieren. Zum Senden von Telemetriedaten ist die Verwendung von KPSN erforderlich.

  Die Konfiguration von Kaspersky Private Security Network ist nur der Web Console oder in der Verwaltungskonsole möglich.

  > Die Konfiguration von KPSN mithilfe der Befehle von Kaspersky Endpoint Security ist nicht verfügbar.

- Aktivieren Sie Komponente "Managed Detection and Response" und laden Sie die BLOB-Konfigurationsdatei, die sich im ZIP-Archiv der MDR-Konfigurationsdatei befindet.

  Sie können die Komponente "Managed Detection and Response" aktivieren und die BLOB-Konfigurationsdatei über die Befehlszeile, in Web Console oder in der Verwaltungskonsole laden.

KPSN für die Integration mit Kaspersky Managed Detection and Response konfigurieren

Sie können die Verwendung von Kaspersky Private Security Network für die Integration mit Kaspersky Managed Detection and Response nur in der Web Console oder in der Verwaltungskonsole konfigurieren.

Um KPSN zu konfigurieren, müssen Sie die Konfigurationsdatei von Kaspersky Security Network (Datei mit der Erweiterung pkcs7), die sich im ZIP-Archiv der MDR-Konfigurationsdatei befindet, auf den Administrationsserver von Kaspersky Security Center hochladen.

Indem Sie die Konfigurationsdatei von Kaspersky Security Network hochladen, erklären Sie sich damit einverstanden, Daten automatisch von einem Gerät mit der installierten App Kaspersky Endpoint Security zur Verarbeitung an Kaspersky zu übermitteln. Laden Sie die Konfigurationsdatei nicht, wenn Sie der Verarbeitung der übermittelten Daten nicht zustimmen. Eine ausführliche Beschreibung der übermittelten Daten finden Sie in der Dokumentation zu Kaspersky Managed Detection and Response.

So konfigurieren Sie KPSN für die Integration von Kaspersky Managed Detection and Response in der Web Console:

1. Öffnen Sie im Hauptfenster von Web Console das Eigenschaftenfenster des Administrationsservers.
2. Wählen Sie in der Liste auf der linken Seite den Abschnitt **Einstellungen des KSN-Proxy-Servers** aus.
3. Aktivieren Sie den Schalter **KSN-Proxy-Server auf dem Administrationsserver aktivieren**, um den Dienst des KSN-Proxy-Servers zu aktivieren.
4. Aktivieren Sie den Schalter **Kaspersky Private Security Network verwenden**.
5. Klicken Sie im Fenster mit der Warnung zu den Besonderheiten der Verwendung des KSN-Proxy-Servers auf Verteilungspunkten mit einer veralteten Version des Administrationsagenten auf die Schaltfläche **OK**.
6. Klicken Sie auf die Schaltfläche **Datei mit den Einstellungen des KSN-Proxy-Servers**.
7. Wählen Sie die Konfigurationsdatei von Kaspersky Security Network (Datei mit der Erweiterung pkcs7) aus und klicken Sie auf **Öffnen**.
8. Klicken Sie auf **Speichern**.

So konfigurieren Sie KPSN für die Integration von Kaspersky Managed Detection and Response in der Verwaltungskonsole:

1. Öffnen Sie in der Struktur der Verwaltungskonsole das Eigenschaftenfenster des Administrationsservers.
2. Wählen Sie den Abschnitt **KSN-Proxy-Server → Einstellungen des KSN-Proxy-Servers** aus.
3. Aktivieren Sie das Kontrollkästchen **Administrationsserver als Proxy-Server verwenden**, um den Dienst des KSN-Proxy-Servers zu aktivieren.
4. Aktivieren Sie das Kontrollkästchen **Private KSN anpassen**.
5. Klicken Sie im Fenster mit der Warnung zu den Besonderheiten der Verwendung des KSN-Proxyservers auf Verteilungspunkten mit einer veralteten Version des Administrationsagenten auf die Schaltfläche **OK**.
6. Klicken Sie auf die Schaltfläche **Datei mit den Einstellungen des KSN-Proxy-Servers**.
7. Wählen Sie die Konfigurationsdatei von Kaspersky Security Network (Datei mit der Erweiterung pkcs7) aus und klicken Sie auf **Öffnen**.
8. Klicken Sie auf **Übernehmen**.

Integration mit Kaspersky Managed Detection and Response in der Web Console konfigurieren

In der Web Console können Sie die Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response in den Richtlinieneinstellungen aktivieren oder deaktivieren und die BLOB-Konfigurationsdatei laden (**App-Einstellungen → Detection and Response → Managed Detection and Response**).

Einstellungen der Integration mit MDR

Einstellung	Beschreibung
Managed Detection and Response aktiviert/deaktiviert	Der Schalter aktiviert oder deaktiviert die Komponente "Managed Detection and Response", die für die Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response erforderlich ist. Der Schalter ist standardmäßig deaktiviert.
Laden	Diese Schaltfläche öffnet ein Standardfenster des Betriebssystems, in dem Sie die BLOB-Konfigurationsdatei auswählen können.

Die BLOB-Konfigurationsdatei befindet sich in einem ZIP-Archiv, das im Lieferumfang der Lösung Kaspersky Managed Detection and Response enthalten ist.

Indem Sie die BLOB-Konfigurationsdatei laden, erklären Sie sich damit einverstanden, Daten automatisch von einem Gerät mit der installierten App Kaspersky Endpoint Security zur Verarbeitung an Kaspersky zu übermitteln. Laden Sie die Konfigurationsdatei nicht, wenn Sie der Verarbeitung der übermittelten Daten nicht zustimmen. Eine ausführliche Beschreibung der übermittelten Daten finden Sie in der Hilfe zu Kaspersky Managed Detection and Response.

Integration mit Kaspersky Managed Detection and Response in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response in den Richtlinieneinstellungen aktivieren oder deaktivieren und die BLOB-Konfigurationsdatei laden (**Detection and Response → Managed Detection and Response**).

Einstellungen der Integration mit MDR

Einstellung	Beschreibung
Managed Detection and Response aktivieren	Das Kontrollkästchen aktiviert die Komponente "Managed Detection and Response", die für die Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response erforderlich ist. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Laden	Diese Schaltfläche öffnet ein Standardfenster von Microsoft Windows, in dem Sie die BLOB-Konfigurationsdatei auswählen können.

Die BLOB-Konfigurationsdatei befindet sich in einem ZIP-Archiv, das im Lieferumfang der Lösung Kaspersky Managed Detection and Response enthalten ist.

Indem Sie die BLOB-Konfigurationsdatei laden, erklären Sie sich damit einverstanden, Daten automatisch von einem Gerät mit der installierten App Kaspersky Endpoint Security zur Verarbeitung an Kaspersky zu übermitteln. Laden Sie die Konfigurationsdatei nicht, wenn Sie der Verarbeitung der übermittelten Daten nicht zustimmen. Eine ausführliche Beschreibung der übermittelten Daten finden Sie in der Hilfe zu Kaspersky Managed Detection and Response.

Integration mit Kaspersky Managed Detection and Response über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie Folgendes tun:

- Die Komponente "Managed Detection and Response" aktivieren oder deaktivieren
- Laden und löschen Sie die für die Integration erforderliche BLOB-Konfigurationsdatei.
- Ändern Sie die Startzeit der Dienstaufgabe *Mdr_Autostart_Scan*, die nach der Integration von Kaspersky Endpoint Security mit Managed Detection and Response automatisch erstellt wird.

Es wird empfohlen, die Konfiguration der Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response in der Verwaltungskonsole oder in der Web Console durchzuführen.

Sie können Managed Detection and Response mithilfe der Option `UseMDR` in den allgemeinen Einstellungen der Anwendung aktivieren oder deaktivieren. Sie können den Wert des Parameters mithilfe von Befehlszeilenschaltern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen App-Einstellungen enthält.

Der Parameter `UseMDR` kann die folgenden Werte annehmen:

- `Yes` – die Komponente "Managed Detection and Response" aktivieren.
- `Nein` – die Komponente "Managed Detection and Response" aktivieren

Sie können die BLOB-Konfigurationsdatei mithilfe der Befehle zur Verwaltung der Lizenzschlüssel laden und löschen.

Führen Sie den folgenden Befehl aus, um die BLOB-Konfigurationsdatei zu laden:

```
kesl-control --load-mdr-blob <Pfad zur BLOB-Konfigurationsdatei von MDR>
```

Führen Sie den folgenden Befehl aus, um die BLOB-Konfigurationsdatei zu löschen:

```
kesl-control --remove-mdr-blob
```

Nach der Aktivierung der Integration wird in der App die Dienstaufgabe *Mdr_Autostart_Scan* erstellt und einmal am Tag ausgeführt. Bei Bedarf können Sie die Startzeit dieser Aufgabe konfigurieren. Andere Aufgabeneinstellungen und die Einstellungen der Aufgabenzeitpläne können nicht geändert werden.

Einstellungen zur Verwendung der App im Light Agent-Modus konfigurieren

Die in diesem Abschnitt beschriebenen Einstellungen können nur angewendet werden, wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird.

Um Kaspersky Endpoint Security im Light Agent-Modus auszuführen, ist eine permanente Interaktion zwischen dem Light Agent und dem auf der SVM installierten Schutzserver erforderlich. Wenn keine Verbindung zum Schutzserver besteht, kann der Light Agent keine Dateifragmente zur Untersuchung an den Schutzserver übertragen und es findet keine Untersuchung statt.

Um mit dem Schutzserver zu interagieren, stellt der Light Agent zu der SVM mit dem installierten Schutzserver eine Verbindung her und erhält diese aufrecht.

Sie können die Einstellungen für die Verbindung des Light Agent mit der SVM in der Web Console oder in der Verwaltungskonsole konfigurieren. Über die Befehlszeile können keine Einstellungen konfiguriert werden; Sie können nur Informationen zur Verwendung der App im Light Agent-Modus anzeigen.

Sie können die folgenden Parameter für die Verbindung von Light Agent mit SVM konfigurieren:

- Methode der SVM-Erkennung. Sie können die Methode auswählen, die von den Light Agents verwendet werden soll, um verfügbare SVMs zum Herstellen einer Verbindung zu erkennen. Der Light Agent kann SVMs, die im Netzwerk ausgeführt werden, auf eine der folgenden Arten erkennen:
  - Mittels des Integrationsservers. SVMs übermitteln Informationen über sich selbst an den Integrationsserver. Der Integrationsserver generiert eine Liste der für die Verbindung verfügbaren SVMs und stellt diese den Light Agents zur Verfügung.

    Um diese Methode der SVM-Erkennung verwenden zu können, müssen die SVMs und Light Agents mit dem Integrationsserver verbunden sein.
  - Mittels einer Liste von SVM-Adressen. Sie können eine Liste mit SVM-Adressen angeben, zu denen die Light Agents eine Verbindung herstellen können.
- Algorithmus zur SVM-Auswahl für die Verbindung. Nachdem der Light Agent Informationen über verfügbare SVMs erhalten hat, wählt er gemäß dem Algorithmus zur SVM-Auswahl die optimale SVM für die Verbindung aus. Sie können angeben, welchen Algorithmus die Light Agents verwenden sollen, wenn sie eine SVM für die Verbindung auswählen.
- Tags der Verbindung. Sie können die Verbindung von Light Agents zur SVM mithilfe von Tags für die Verbindung regulieren. Wenn Sie für eine Verbindung Tags verwenden, kann der Light Agent nur eine Verbindung zu den SVMs herstellen, auf denen die Verwendung dieses Tags zur Verbindung konfiguriert ist.
- Schutz der Verbindung zwischen dem Light Agent und dem Schutzserver. Sie können die Verbindung zwischen Light Agents und Schutzservern durch Verschlüsselung schützen.

Weitere Informationen zu den Verbindungseinstellungen zwischen einem Light Agent und SVMs finden Sie in der Hilfe der zu Kaspersky Security for Virtualization Light Agent.

Light Agent-Einstellungen in der Web Console konfigurieren

In der Web Console können Sie die Einstellungen für die Verbindung des Light Agents mit der SVM in den Richtlinieneinstellungen konfigurieren (**App-Einstellungen** → **Light Agent-Modus**).

Einstellungen der SVM-Erkennung

Die in diesem Abschnitt beschriebenen Einstellungen können nur angewendet werden, wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird.

In diesem Fenster können Sie die Methode auswählen, die von den Light Agents verwendet werden soll, um für verfügbare SVMs zum Herstellen einer Verbindung zu erkennen:

Einstellungen der SVM-Erkennung

Einstellung	Beschreibung
Integrationsserver verwenden	Wenn diese Option ausgewählt ist, stellt der Light Agent eine Verbindung zum Integrationsserver her, um eine Liste der für die Verbindung verfügbaren SVMs und Informationen darüber zu erhalten. Wenn Sie den Integrationsserver verwenden möchten, müssen Sie die Einstellungen für die Verbindung von Light Agents mit dem Integrationsserver konfigurieren.
Manuell hinzugefügte Liste mit SVM-Adressen verwenden	Wenn diese Option ausgewählt ist, können Sie eine Liste von SVMs angeben, mit denen Light Agents, die durch diese Richtlinie verwaltet werden, eine Verbindung herstellen können. Die Light Agents stellen nur Verbindungen zu den in der Liste angegebenen SVMs her.
Liste der SVM-Adressen	Eine Liste mit IP-Adressen im IPv4-Format oder vollqualifizierten Domänennamen (FQDN) der SVMs, mit denen die Light Agents, die durch die Richtlinie verwaltet werden, eine Verbindung herstellen können. Durch Klicken auf die Schaltfläche **Hinzufügen** öffnet sich ein Fenster, in dem Sie die IP-Adresse im IPv4-Format oder den vollqualifizierten Domänennamen (FQDN) der SVM angeben können. Sie können IP-Adressen oder vollqualifizierte Domänennamen von SVMs in einer neuen Zeile eingeben. Es können nur vollqualifizierte Domänennamen (FQDNs) angeben werden, die jeweils einer einzelnen IP-Adresse entsprechen. Die Verwendung eines vollständig qualifizierten Domänennamens, der mehreren IP-Adressen entspricht, kann zu Fehlern in der App führen. Sie können in der Liste ausgewählte Adressen löschen, indem Sie auf die Schaltfläche **Löschen** klicken. Wenn die Option **Manuell hinzugefügte Liste mit SVM-Adressen verwenden** ausgewählt ist, wird die Liste der SVM-Adressen wird angezeigt, ist.

Wenn Sie die Option **Manuell hinzugefügte Liste mit SVM-Adressen verwenden** ausgewählt haben und für den Light Agent der erweiterte Algorithmus zur SVM-Auswahl verwendet wird sowie auf der SVM der Modus zum Schutz großer Infrastrukturen aktiviert ist (mehr dazu finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent), dann ist die Verbindung eines Light Agents mit dieser SVM nur möglich, wenn der Standort der SVM nicht berücksichtigt wird. Im Abschnitt **Algorithmus zur SVM-Auswahl** müssen Sie die Option **SVM-Standort** auf **SVM-Standort ignorieren** festlegen. Bei einem beliebigen anderen angegebenen Wert kann der Light Agent keine Verbindung zur SVM herstellen.

Einstellung der Verbindung zum Integrationsserver

Die in diesem Abschnitt beschriebenen Einstellungen können nur angewendet werden, wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird.

Wenn Sie möchten, dass die Light Agents Informationen über die SVMs mittels des Integrationsservers erhalten, oder wenn Sie die Verbindung zwischen dem Schutzserver und dem Light Agent sichern möchten, ist eine Verbindung zum Integrationsserver erforderlich.

In diesem Fenster werden die aktuellen Parameter für die Verbindung von Light Agents mit dem Integrationsserver angezeigt: Adresse und Port für die Verbindung. Durch Klicken auf die Schaltfläche **Ändern** öffnet sich das Fenster **Verbindung zum Integrationsserver**, in dem Sie die Verbindung zum Integrationsserver konfigurieren können.

Fenster "Verbindung zum Integrationsserver"

In diesem Fenster können Sie die Parameter für die Verbindung von Light Agents mit dem Integrationsserver festlegen oder ändern.

Einstellung der Verbindung zum Integrationsserver

Einstellung	Beschreibung
Adresse	IP-Adresse im IPv4-Format oder als vollqualifizierter Domänenname (FQDN) des Geräts mit installiertem Integrationsserver. Wenn als Adresse der NetBIOS-Name, "localhost" oder "127.0.0.1" angegeben wird, schlägt die Verbindung zum Integrationsserver mit einem Fehler fehl.
Port	Port für die Verbindung zum Integrationsserver. Standardmäßig ist Port 7271 angegeben.
Untersuchen	Wenn Sie auf die Schaltfläche klicken, prüft das Web-Plug-in das vom Integrationsserver empfangene SSL-Zertifikat. Die Schaltfläche ist nach Eingabe der Adresse und des Ports für die Verbindung mit dem Integrationsserver zur Verfügung. Wenn das Zertifikat einen Fehler enthält oder nicht vertrauenswürdig ist, wird im Fenster **Verbindung zum Integrationsserver** eine entsprechende Meldung angezeigt.
Vertrauenswürdiges Zertifikat anzeigen	Durch Anklicken der Zeile können Sie Informationen über das vom Integrationsserver erhaltene Zertifikat anzeigen.

Ignorieren	Wählen Sie diese Option, um das erhaltene Zertifikat zu speichern und die Verbindung zum Integrationsserver fortzusetzen. Falls Probleme mit einem SSL-Zertifikat auftreten, empfiehlt es sich, sicherzustellen, dass der von Ihnen verwendete Kanal zur Datenübertragung sicher ist.
Abbrechen	Wählen Sie diese Option, um das Herstellen einer Verbindung zum Integrationsserver zu beenden.
Kennwort	Kennwort für das Administratorkonto des Integrationsservers (Kennwort des Kontos "admin"). Es wird empfohlen, sicherzustellen, dass die Passwortkomplexität und die Anti-Brute-Force-Mechanismen gewährleisten, dass das Passwort innerhalb von 6 Monaten nicht geknackt werden kann.
Untersuchen	Durch Klicken auf die Schaltfläche verbindet sich das Web-Plug-in mit dem Integrationsserver. Nachdem die Verbindung mit Integrationsserver mittels Administratorrechten hergestellt wurde, wird das Kennwort Benutzerkontos "agent" automatisch in die Richtlinie übertragen, die zur Verbindung von Light Agents mit dem Integrationsserver verwendet wird. Das Kennwort wird verschlüsselt gespeichert.

Tag der Verbindung zur SVM

In diesem Fenster können Sie dem Light Agent die Verwendung von Tags ermöglichen und ein Tag zuweisen, das der Light Agent für die Verbindung verwendet.

Stellen Sie sicher, dass die Verwendung von Tags für Verbindungen auch in den Einstellungen des Schutzservers konfiguriert ist: Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent. Light Agents, denen ein Tag zugewiesen wurde, können sich nur mit SVMs verbinden, denen die Verbindung mit Light Agents mit diesem Tag erlaubt ist.

Optionen zur Verwendung von Tags für die Verbindung

Einstellung	Beschreibung
Tags für die Verbindung von Light Agents verwenden	Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung von Tags durch den Light Agent für die Verbindung zur SVM.
Tag	Ein Tag, das den Light Agents zugewiesen ist. Als Tag kann eine bis zu 255 Zeichen lange Zeichenkette eingegeben werden. Sie können jedes Zeichen mit Ausnahme von `;` verwenden. Das Feld ist verfügbar, wenn das Kontrollkästchen **Tags für die Verbindung von Light Agents verwenden** aktiviert ist.

Algorithmus der SVM-Auswahl

In diesem Fenster können Sie angeben, welchen Algorithmus zur SVM-Auswahl die Light Agents für Linux verwenden sollen, und die Einstellungen für die Verwendung des erweiterten Algorithmus zur SVM-Auswahl konfigurieren.

Algorithmus der SVM-Auswahl

Einstellung	Beschreibung
Standard-Algorithmus zur SVM-Auswahl verwenden	Wenn diese Option ausgewählt ist, wählt ein Light Agent nach der Installation und Ausführung auf einer virtuellen Maschine die Verbindung zu einer SVM, die für Light Agent lokal ist. Weitere Informationen finden Sie in der Hilfe von Kaspersky Security for Virtualization Light Agent. Wenn keine lokalen SVMs für die Verbindung verfügbar sind, wählt der Light Agent unabhängig vom Standort der SVMs in der virtuellen Infrastruktur die SVM aus, mit der die wenigsten Light Agents verbunden sind. Diese Option ist standardmäßig ausgewählt.
Erweiterten Algorithmus zur SVM-Auswahl verwenden	Wenn diese Option ausgewählt ist, können Sie mit dem Schieberegler **SVM-Standort** festlegen, inwieweit der SVM-Standort in der virtuellen Infrastruktur eine Rolle bei der Bestimmung des lokalen Standorts der SVM relativ zum Light Agent berücksichtigt wird. Der Light Agent kann nur eine Verbindung zu SVMs herstellen, die für den Light Agent lokal sind. Sie können auch festlegen, dass der SVM-Standort in der virtuellen Infrastruktur bei der Auswahl einer SVM für die Verbindung nicht berücksichtigt werden soll. Bei der Auswahl einer SVM berücksichtigen Light Agents die Anzahl der mit dieser SVM verbundenen weiteren Light Agents, um eine gleichmäßige Verteilung der Light Agents auf die verfügbaren SVMs für die Verbindung sicherzustellen.
SVM-Standort	Ermöglicht Ihnen, den Standorttyp der SVM in der virtuellen Infrastruktur anzugeben, der bei der Auswahl einer SVM für die Verbindung berücksichtigt wird: • **Hypervisor**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur): ◦ Die SVM wird auf demselben Hypervisor bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, Alt Virtualization Server, Astra Linux oder Numa vServer). ◦ Die SVM befindet sich in derselben Servergruppe wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen unter Verwaltung von OpenStack, VK Cloud Platform oder TIONICS Cloud Platform). Wenn auf demselben Hypervisor oder in derselben Servergruppe, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her. • **Cluster**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur): ◦ Die SVM wird auf demselben Hypervisor-Cluster bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Scala-R), HUAWEI FusionSphere, Nutanix Acropolis, Alt Virtualization Server, Astra Linux oder Numa vServer).

- Die SVM wird innerhalb desselben OpenStack-Projekts bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen unter Verwaltung von OpenStack, VK Cloud Platform oder TIONICS Cloud Platform).

Wenn auf demselben Hypervisor-Cluster oder innerhalb eines OpenStack-Projektes, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her.

- **Rechenzentrum**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):

  - Die SVM wird im selben Rechenzentrum bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Scala-R), HUAWEI FusionSphere, Nutanix Acropolis, Alt Virtualization Server, Astra Linux oder Numa vServer).

  - Die SVM befindet sich in derselben Verfügbarkeitszone wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen unter Verwaltung von OpenStack, VK Cloud Platform oder TIONICS Cloud Platform).

Wenn in demselben Rechenzentrum oder in derselben Verfügbarkeitszone, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her.

- **SVM-Standort ignorieren**. Der Light Agent berücksichtigt bei der Auswahl einer SVM ihren Standort nicht.

Standardmäßig ist der Wert **Hypervisor** ausgewählt.

Die Option ist verfügbar, wenn die Option **Erweiterten Algorithmus zur SVM-Auswahl verwenden** ausgewählt ist.

Wenn für den Light Agent der erweiterte Algorithmus zur SVM-Auswahl verwendet wird, als Methode zur SVM-Erkennung die Liste mit SVM-Adressen ausgewählt ist und auf der SVM der Modus zum Schutz großer Infrastrukturen aktiviert ist (mehr dazu finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent), dann ist die Verbindung des Light Agents mit dieser SVM nur möglich, wenn der Standort der SVM nicht berücksichtigt wird. Sie müssen der Wert des Parameters **SVM-Standort** auf **SVM-Standort ignorieren** setzen. Bei einem beliebigen anderen angegebenen Wert kann der Light Agent keine Verbindung zur SVM herstellen.

Verbindung absichern

In diesem Fenster können Sie die Verschlüsselung für den Kanal zur Datenübertragung zwischen dem Light Agent und dem Schutzserver aktivieren.

Stellen Sie sicher, dass die Verschlüsselung des Datenübertragungskanals zwischen dem Light Agent und dem Schutzserver in den Einstellungen des Schutzservers auf der SVM aktiviert ist. Weitere Informationen finden Sie in der Hilfe von Kaspersky Security for Virtualization Light Agent.

Schutz-Einstellungen für die Verbindung

Einstellung	Beschreibung
Datenübertragungskanal	Sichern Sie die Verbindung zwischen Light Agents und dem Schutzserver durch

zwischen dem Light Agent und dem Schutzserver verschlüsseln	Verschlüsselung ab. Bei aktivierten Kontrollkästchen wird eine sichere Verbindung zwischen dem Light Agent, der unter Verwaltung der Richtlinie steht, und dem Schutzserver auf der SVM, mit der sich der Light Agent verbindet, hergestellt. Ein Light Agent, für den der Schutz der Verbindung aktiviert ist, kann nur eine Verbindung zu einer SVM herstellen, für die ebenfalls der Schutz der Verbindung aktiviert ist oder die ungesicherte Verbindungen zum Schutzserver zulässt. Bei aktivierten Kontrollkästchen wird eine ungesicherte Verbindung zwischen dem Light Agent und dem Schutzserver auf der SVM, mit der sich der Light Agent verbindet, hergestellt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Light Agent-Einstellungen in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen für die Verbindung des Light Agents mit der SVM in den Richtlinieneinstellungen konfigurieren (**Light Agent-Modus**).

Verbindung zum Integrationsserver

Die in diesem Abschnitt beschriebenen Einstellungen können nur angewendet werden, wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird.

Wenn Sie möchten, dass die Light Agents Informationen über die SVMs mittels des Integrationsservers erhalten, oder wenn Sie die Verbindung zwischen dem Schutzserver und dem Light Agent sichern möchten, ist eine Verbindung zum Integrationsserver erforderlich.

In diesem Fenster werden die aktuellen Parameter für die Verbindung von Light Agents mit dem Integrationsserver angezeigt: Adresse und Port für die Verbindung. Durch Klicken auf die Schaltfläche **Ändern** öffnet sich das Fenster **Verbindung zum Integrationsserver**, in dem Sie die Verbindung zum Integrationsserver konfigurieren können.

Fenster "Verbindung zum Integrationsserver"

In diesem Fenster können Sie die Parameter für die Verbindung von Light Agents mit dem Integrationsserver festlegen oder ändern.

Einstellung der Verbindung zum Integrationsserver

Einstellung	Beschreibung
Adresse	IP-Adresse im IPv4-Format oder als vollqualifizierter Domänenname (FQDN) des Geräts mit installiertem Integrationsserver. Wenn das Gerät mit installierter Kaspersky Security Center Verwaltungskonsole zu einer Domäne gehört, wird in dem Feld standardmäßig der Domänenname des Geräts angegeben. Wenn das Gerät mit installierter Kaspersky Security Center Verwaltungskonsole in keiner Domäne enthalten ist oder der Integrationsserver auf einem anderen Gerät installiert ist, muss das Feld manuell ausgefüllt werden.

	Wenn als Adresse der NetBIOS-Name, "localhost" oder "127.0.0.1" angegeben wird, schlägt die Verbindung zum Integrationsserver mit einem Fehler fehl.
Port	Port für die Verbindung zum Integrationsserver. Standardmäßig ist Port 7271 angegeben.

Fenster "Überprüfung des Zertifikats vom Integrationsserver"

Dieses Fenster wird angezeigt, wenn das vom Integrationsserver empfangene SSL-Zertifikat einen Fehler enthält oder nicht vertrauenswürdig ist.

Über den Link im Fenster können Sie Informationen zum erhaltenen Zertifikat anzeigen.

Falls Probleme mit einem SSL-Zertifikat auftreten, empfiehlt es sich, sicherzustellen, dass der von Ihnen verwendete Kanal zur Datenübertragung sicher ist.

Um die Herstellung der Verbindung zum Integrationsserver fortzusetzen, klicken Sie auf die Schaltfläche **Ignorieren**. Das empfangene Zertifikat wird als vertrauenswürdiges Zertifikat auf dem Gerät mit installierter Kaspersky Security Center Verwaltungskonsole installiert.

Fenster "Authentifizierung auf dem Integrationsserver"

Dieses Fenster wird angezeigt, wenn das Gerät mit installierter Kaspersky Security Center Verwaltungskonsole nicht Teil einer Domäne ist oder Ihr Konto kein Mitglied in einer der folgenden Gruppen ist: lokalen Gruppe "KLAdmins", Domänengruppe "KLAdmins" oder lokale Administratorengruppe.

Geben Sie das Administratorkennwort des Integrationsservers (Kennwort des Kontos `admin`) an und klicken Sie auf die Schaltfläche **OK**.

Es wird empfohlen, sicherzustellen, dass die Passwortkomplexität und die Anti-Brute-Force-Mechanismen gewährleisten, dass das Passwort innerhalb von 6 Monaten nicht geknackt werden kann.

Nachdem die Verbindung mit Integrationsserver mittels Administratorrechten hergestellt wurde, wird das Kennwort Benutzerkontos `agent` automatisch in die Richtlinie übertragen, die zur Verbindung von Light Agents mit dem Integrationsserver verwendet wird.

Einstellungen der SVM-Erkennung

Die in diesem Abschnitt beschriebenen Einstellungen können nur angewendet werden, wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird.

In diesem Fenster können Sie die Methode auswählen, die von den Light Agents verwendet werden soll, um für verfügbare SVMs zum Herstellen einer Verbindung zu erkennen:

Einstellung	Beschreibung
Integrationsserver verwenden	Wenn diese Option ausgewählt ist, stellt der Light Agent eine Verbindung zum Integrationsserver her, um eine Liste der für die Verbindung verfügbaren SVMs und Informationen darüber zu erhalten. Wenn Sie den Integrationsserver verwenden möchten, müssen Sie die Einstellungen für die Verbindung von Light Agents mit dem Integrationsserver konfigurieren.
Manuell hinzugefügte Liste mit SVM-Adressen verwenden	Wenn diese Option ausgewählt ist, können Sie eine Liste von SVMs angeben, mit denen Light Agents, die durch diese Richtlinie verwaltet werden, eine Verbindung herstellen können. Die Light Agents stellen nur Verbindungen zu den in der Liste angegebenen SVMs her.
Liste der SVMs	Eine Liste mit IP-Adressen im IPv4-Format oder vollqualifizierten Domänennamen (FQDN) der SVMs, mit denen die Light Agents, die durch die Richtlinie verwaltet werden, eine Verbindung herstellen können. Durch Klicken auf die Schaltfläche **Hinzufügen** öffnet sich ein Fenster, in dem Sie die IP-Adresse im IPv4-Format oder den vollqualifizierten Domänennamen (FQDN) der SVM angeben können. Sie können IP-Adressen oder vollqualifizierte Domänennamen von SVMs in einer neuen Zeile eingeben. Es können nur vollqualifizierte Domänennamen (FQDNs) angeben werden, die jeweils einer einzelnen IP-Adresse entsprechen. Die Verwendung eines vollständig qualifizierten Domänennamens, der mehreren IP-Adressen entspricht, kann zu Fehlern in der App führen. Sie können in der Liste ausgewählte Adressen löschen, indem Sie auf die Schaltfläche **Löschen** klicken. Wenn die Option **Manuell hinzugefügte Liste mit SVM-Adressen verwenden** ausgewählt ist, wird die Liste der SVM-Adressen wird angezeigt, ist.

Wenn Sie die Option **Manuell hinzugefügte Liste mit SVM-Adressen verwenden** ausgewählt haben und für den Light Agent der erweiterte Algorithmus zur SVM-Auswahl verwendet wird sowie auf der SVM der Modus zum Schutz großer Infrastrukturen aktiviert ist (mehr dazu finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent), dann ist die Verbindung eines Light Agents mit dieser SVM nur möglich, wenn der Standort der SVM nicht berücksichtigt wird. Im Abschnitt **Algorithmus zur SVM-Auswahl** müssen Sie die Option **SVM-Standort** auf **SVM-Standort ignorieren** festlegen. Bei einem beliebigen anderen angegebenen Wert kann der Light Agent keine Verbindung zur SVM herstellen.

Tag der Verbindung zur SVM

In diesem Fenster können Sie dem Light Agent die Verwendung von Tags ermöglichen und ein Tag zuweisen, das der Light Agent für die Verbindung verwendet.

Stellen Sie sicher, dass die Verwendung von Tags für Verbindungen auch in den Einstellungen des Schutzservers konfiguriert ist: Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent. Light Agents, denen ein Tag zugewiesen wurde, können sich nur mit SVMs verbinden, denen die Verbindung mit Light Agents mit diesem Tag erlaubt ist.

Optionen zur Verwendung von Tags für die Verbindung

Einstellung	Beschreibung
Tags für die Verbindung von Light Agents verwenden	Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung von Tags durch den Light Agent für die Verbindung zur SVM.
Tag	Ein Tag, das den Light Agents zugewiesen ist. Als Tag kann eine bis zu 255 Zeichen lange Zeichenkette eingegeben werden. Sie können jedes Zeichen mit Ausnahme von `;` verwenden. Das Feld ist verfügbar, wenn das Kontrollkästchen **Tags für die Verbindung von Light Agents verwenden** aktiviert ist.

Algorithmus der SVM-Auswahl

In diesem Fenster können Sie angeben, welchen Algorithmus zur SVM-Auswahl die Light Agents für Linux verwenden sollen, und die Einstellungen für die Verwendung des erweiterten Algorithmus zur SVM-Auswahl konfigurieren.

Algorithmus der SVM-Auswahl

Einstellung	Beschreibung
Standard-Algorithmus zur SVM-Auswahl verwenden	Wenn diese Option ausgewählt ist, wählt ein Light Agent nach der Installation und Ausführung auf einer virtuellen Maschine die Verbindung zu einer SVM, die für Light Agent lokal ist. Weitere Informationen finden Sie in der Hilfe von Kaspersky Security for Virtualization Light Agent. Wenn keine lokalen SVMs für die Verbindung verfügbar sind, wählt der Light Agent unabhängig vom Standort der SVMs in der virtuellen Infrastruktur die SVM aus, mit der die wenigsten Light Agents verbunden sind. Diese Option ist standardmäßig ausgewählt.
Erweiterten Algorithmus zur SVM-Auswahl verwenden	Wenn diese Option ausgewählt ist, können Sie mit dem Schieberegler **SVM-Standort** festlegen, inwieweit der SVM-Standort in der virtuellen Infrastruktur eine Rolle bei der Bestimmung des lokalen Standorts der SVM relativ zum Light Agent berücksichtigt wird. Der Light Agent kann nur eine Verbindung zu SVMs herstellen, die für den Light Agent lokal sind. Sie können auch festlegen, dass der SVM-Standort in der virtuellen Infrastruktur bei der Auswahl einer SVM für die Verbindung nicht berücksichtigt werden soll. Bei der Auswahl einer SVM berücksichtigen Light Agents die Anzahl der mit dieser SVM verbundenen weiteren Light Agents, um eine gleichmäßige Verteilung der Light Agents auf die verfügbaren SVMs für die Verbindung sicherzustellen.
SVM-Standort	Ermöglicht Ihnen, den Standorttyp der SVM in der virtuellen Infrastruktur anzugeben, der bei der Auswahl einer SVM für die Verbindung berücksichtigt wird: • **Hypervisor**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur): ◦ Die SVM wird auf demselben Hypervisor bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Microsoft

Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, Alt Virtualization Server, Astra Linux oder Numa vServer).

- Die SVM befindet sich in derselben Servergruppe wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen unter Verwaltung von OpenStack, VK Cloud Platform oder TIONICS Cloud Platform).

Wenn auf demselben Hypervisor oder in derselben Servergruppe, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her.

- **Cluster**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):

  - Die SVM wird auf demselben Hypervisor-Cluster bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Scala-R), HUAWEI FusionSphere, Nutanix Acropolis, Alt Virtualization Server, Astra Linux oder Numa vServer).

  - Die SVM wird innerhalb desselben OpenStack-Projekts bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen unter Verwaltung von OpenStack, VK Cloud Platform oder TIONICS Cloud Platform).

Wenn auf demselben Hypervisor-Cluster oder innerhalb eines OpenStack-Projektes, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her.

- **Rechenzentrum**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):

  - Die SVM wird im selben Rechenzentrum bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Scala-R), HUAWEI FusionSphere, Nutanix Acropolis, Alt Virtualization Server, Astra Linux oder Numa vServer).

  - Die SVM befindet sich in derselben Verfügbarkeitszone wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen unter Verwaltung von OpenStack, VK Cloud Platform oder TIONICS Cloud Platform).

Wenn in demselben Rechenzentrum oder in derselben Verfügbarkeitszone, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her.

- **SVM-Standort ignorieren**. Der Light Agent berücksichtigt bei der Auswahl einer SVM ihren Standort nicht.

Standardmäßig ist der Wert **Hypervisor** ausgewählt.

Die Option ist verfügbar, wenn die Option **Erweiterten Algorithmus zur SVM-Auswahl verwenden** ausgewählt ist.

Wenn für den Light Agent der erweiterte Algorithmus zur SVM-Auswahl verwendet wird, als Methode zur SVM-Erkennung die Liste mit SVM-Adressen ausgewählt ist und auf der SVM der Modus zum Schutz großer Infrastrukturen aktiviert ist (mehr dazu finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent), dann ist die Verbindung des Light Agents mit dieser SVM nur möglich, wenn der Standort der SVM nicht berücksichtigt wird. Sie müssen der Wert des Parameters **SVM-Standort** auf **SVM-Standort ignorieren** setzen. Bei einem beliebigen anderen angegebenen Wert kann der Light Agent keine Verbindung zur SVM herstellen.

Verbindung absichern

In diesem Fenster können Sie die Verschlüsselung für den Kanal zur Datenübertragung zwischen dem Light Agent und dem Schutzserver aktivieren.

Stellen Sie sicher, dass die Verschlüsselung des Datenübertragungskanals zwischen dem Light Agent und dem Schutzserver in den Einstellungen des Schutzservers auf der SVM aktiviert ist. Weitere Informationen finden Sie in der Hilfe von Kaspersky Security for Virtualization Light Agent.

Schutz-Einstellungen für die Verbindung

Einstellung	Beschreibung
Datenübertragungskanal zwischen dem Light Agent und dem Schutzserver verschlüsseln	Sichern Sie die Verbindung zwischen Light Agents und dem Schutzserver durch Verschlüsselung ab. Bei aktivierten Kontrollkästchen wird eine sichere Verbindung zwischen dem Light Agent, der unter Verwaltung der Richtlinie steht, und dem Schutzserver auf der SVM, mit der sich der Light Agent verbindet, hergestellt. Ein Light Agent, für den der Schutz der Verbindung aktiviert ist, kann nur eine Verbindung zu einer SVM herstellen, für die ebenfalls der Schutz der Verbindung aktiviert ist oder die ungesicherte Verbindungen zum Schutzserver zulässt. Bei aktivierten Kontrollkästchen wird eine ungesicherte Verbindung zwischen dem Light Agent und dem Schutzserver auf der SVM, mit der sich der Light Agent verbindet, hergestellt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Informationen zur Verwendung der App im Light Agent-Modus über die Befehlszeile anzeigen

In der Befehlszeile können Sie die folgenden Informationen zur Verwendung der App im Light Agent-Modus zum Schutz virtueller Umgebungen anzeigen:

- Einstellungen zur Verwendung der App im Light Agent-Modus;
- Verbindung des Light Agents zum Integrationsserver;
- Verbindung des Light Agents zur SVM.

Um Informationen zu den Einstellungen für die Verwendung der App im Light Agent-Modus anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control [-V] --ksvla-info
```

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

- Light Agent-Modus zum Schutz virtueller Umgebungen: aktiviert/deaktiviert.

  Wenn der Light Agent-Modus aktiviert ist, wird die App als Light Agent im Rahmen von Kaspersky Security for Virtualization Light Agent verwendet. Wenn der Light Agent-Modus deaktiviert ist, wird die App im Standard-Modus verwendet.

- Modus zum Schutz der VDI-Infrastruktur: aktiviert/deaktiviert.

  Der Modus zum Schutz der VDI-Infrastruktur optimiert die Ausführung von Kaspersky Endpoint Security auf temporären virtuellen Maschinen. Wenn der Modus zum Schutz der VDI-Infrastruktur aktiviert ist, werden Updates, die einen Neustart der geschützten virtuellen Maschine erfordern, nicht auf temporären virtuellen Maschinen installiert. Wenn Updates eingehen, die einen Neustart erfordern, sendet der auf einer temporären virtuellen Maschine installierte Light Agent eine Nachricht an Kaspersky Security Center über die Notwendigkeit, die Vorlage der geschützte virtuellen Maschinen zu aktualisieren.

- Typ der geschützten virtuellen Maschine: temporär oder permanent.

- Rolle der geschützten virtuellen Maschine in der virtuellen Infrastruktur: Server oder Workstation.

- ID/Identifikator (UUID) der geschützten virtuellen Maschine.

Um Informationen zur Verbindung des Light Agents mit dem Integrationsserver anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control [-V] --viis-info
```

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

- Adresse und der Port des Integrationsservers, mit dem sich der Light Agent verbindet.

- Status der Verbindung zum Integrationsserver.

- Datum und Uhrzeit der letzten Verbindung zwischen dem Light Agent und dem Integrationsserver.

Um Informationen zur Verbindung des Light Agents mit der SVM anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control [-V] --svm-info
```

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

- Die Adresse der SVM, mit welcher der Light Agent verbunden ist, und der SVM-Standort in der virtuellen Infrastruktur relativ zum Light Agent: lokal oder nicht lokal.

- Methode der SVM-Erkennung des Light Agents: mittels Integrationsservers oder mittels manuell angegebener Liste von SVM-Adressen.

- Liste der SVM-Adressen, wenn als Methode der SVM-Erkennung die Liste von SVM-Adressen ausgewählt ist.

- Tag der Verbindung von Light Agent zur SVM.

- Algorithmus zur SVM-Auswahl: Standard oder erweitert. Bei Verwendung des erweiterten Algorithmus zur SVM-Auswahl wird auch der SVM-Standort in der virtuellen Infrastruktur angezeigt.

- Vorhandener Schutz für die Verbindung zwischen dem Light Agent und dem Schutzserver.

Weitere Informationen zu den Verbindungseinstellungen zwischen Light Agents und Integrationsserver bzw. SVMs finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

Ereignisse und Berichte anzeigen

Während der Ausführung der App können unterschiedliche *Ereignisse* ausgelöst werden. Diese können rein informativ sein oder wichtige Informationen enthalten. Die App kann beispielsweise mithilfe von Ereignissen über erfolgreiche Updates der App-Datenbanken informieren oder auf eine Funktionsstörung einer Komponente hinweisen, die behoben werden muss.

Mit Kaspersky Endpoint Security können Sie Informationen über Ereignisse, die während der App-Ausführung auftreten, in die folgenden Protokolle eintragen:

- Ereignisprotokoll der App. Standardmäßig speichert die App die Informationen über Ereignisse in der Datenbank /var/opt/kaspersky/kesl/private/storage/events.db. Sie können die Einstellungen des Ereignisprotokolls der App über die Befehlszeile konfigurieren.
- Protokoll des Betriebssystems (Syslog). Standardmäßig wird das Protokoll des Betriebssystems nicht verwendet. Sie können die Ereignisprotokollierung in diesem Protokoll aktivieren.

Für den Zugriff auf das Ereignisprotokoll der App und das Protokoll des Betriebssystems sind Root-Rechte erforderlich.

Wenn Kaspersky Endpoint Security über Kaspersky Security Center verwaltet wird, werden möglicherweise Informationen zu Ereignissen an den Administrationsserver von Kaspersky Security Center übertragen. Für einige Ereignisse gelten Aggregationsregeln. Wenn während der Nutzung der App in kurzer Zeit viele Ereignisse desselben Typs generiert werden, wechselt die App in den Ereignisaggregationsmodus und sendet ein aggregiertes Ereignis mit einer Beschreibung der Parameter dieser Ereignisse an Kaspersky Security Center. Für unterschiedliche Ereignisse können unterschiedliche Aggregationsregeln verwendet werden. Nähere Informationen zu Ereignissen finden Sie in der Hilfe zu Kaspersky Security Center.

Sie können Informationen zu App-Ereignissen auf folgende Arten abrufen:

- In der Verwaltungskonsole und in der Web Console.
- Über die Befehlszeile.
- In Pop-ups der App, wenn Sie die grafische Benutzeroberfläche von Kaspersky Endpoint Security verwenden.

Einige Ereignisse können Dateipfade enthalten. Bei der Ausgabe wird der Dateipfad als String mit UTF-8-Encoding behandelt. Wenn eines der Bytes im Pfad nicht den Regeln des UTF-8-Encodings entspricht, wird es durch das Zeichen `?` ersetzt. Durch das Symbol `?` werden auch Abfolgen von vier Bytes ersetzt, die den Code von Zeichen außerhalb des Unicode-Bereichs (größer als 0x10FFFF) kodieren. Sonderzeichen werden auf eine bestimmte Weise maskiert (ersetzt).

Regeln für das Escape-Zeichen in Dateipfaden in Ereignissen, wenn diese mit dem Befehl `kesl-control -E --query` ausgegeben werden:

- Die Zeichen '\a', '\b', '\t', '\n', '\v', '\f', '\r' werden wie folgt durch zwei Zeichen ersetzt:

  '\a' -> "\\a"

  '\b' -> "\\b"

  '\t' -> "\\t"

  '\n' -> "\\n"

  '\v' -> "\\v"

  '\f' -> "\\f"

  '\r' -> "\\r"

- Alle weiteren Sonderzeichen werden unverändert ausgegeben.

Regeln für das Escape-Zeichen in Dateipfaden in Ereignissen, wenn diese mit dem Befehl `kesl-control -E --query --json` ausgegeben werden:

- Die Zeichen '\b', '\f', '\n', '\r', '\t' '"', '\\' werden entsprechend dem JSON-Format wie folgt maskiert:

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

  '"' -> "\\\""

  '\\' -> "\\\\"

- Alle anderen Sonderzeichen werden entsprechend den allgemeinen Escape-Regeln für Sonderzeichen des JSON-Formats maskiert ('\a' -> '\u0007').

Regeln für Escape-Zeichen in Dateipfaden in Ereignissen beim der Übertragung an syslog:

- Die Zeichen '\b', '\f', '\n', '\r', '\t' '"', '\\' werden entsprechend dem JSON-Format wie folgt maskiert:

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

  '"' -> "\\\""

  '\\' -> "\\\\"

- Alle anderen Sonderzeichen werden entsprechend den allgemeinen Escape-Regeln für Sonderzeichen des JSON-Formats maskiert ('\a' -> '\u0007').

Der erste Backslash in der Reihenfolge bei der Beschreibung von Regeln stellt jeweils ein Escape-Zeichen dar.

Beispiele:
`'\a'` ist ein Zeichen (maskierter Buchstabe)

`'\\a'` sind zwei Zeichen (Backslash + a)

`'\\'` ist ein Zeichen (Backslash) – `'\\\\'` sind zwei Zeichen (Backslash + Backslash).

Auf Basis der Ereignisse, die während der Ausführung der App eintreten, können verschiedene Arten von *Berichten* erstellt werden. Informationen zur Ausführung jeder Komponente von Kaspersky Endpoint Security, zur Ausführung aller Aufgaben und zur allgemeinen Ausführung der App werden in Berichten aufgezeichnet.

Berichte können wie folgt angezeigt werden:

- Berichte von Kaspersky Security Center sind in der Verwaltungskonsole und in der Web Console verfügbar. Mit diesen Berichten können Sie z. B. Informationen über infizierte Dateien sowie die Verwendung von Schlüsseln und App-Datenbanken erhalten. Nähere Informationen über die Verwendung der Berichte von Kaspersky Security Center finden Sie in der Hilfe zu Kaspersky Security Center.

- App-Berichte sind in der grafischen Benutzeroberfläche von Kaspersky Endpoint Security verfügbar.

Ereignisse und Berichte können die folgenden persönlichen Daten enthalten:

- Namen und IDs der Benutzer im Betriebssystem
- Pfade der Benutzerdateien
- IP-Adressen der Remote-Geräte, die von der Komponente Schutz vor Verschlüsselung untersucht werden
- IP-Adressen der Sender und Empfänger der Netzwerkpakete, die von der Komponente Firewall-Verwaltung untersucht werden
- Webadressen der Update-Quellen
- Werte der allgemeinen App-Einstellungen
- Namen und Einstellungen von Befehlszeilenaufgaben
- Erkannte bösartige Webadressen, Phishing- und Adware-Adressen sowie Webadressen, die legale Anwendungen enthalten, mit der Kriminelle Ihre Geräte oder Ihre persönlichen Daten beschädigen können
- Namen der Container und Images
- Pfade zu den Containern und Images
- Namen und IDs der Geräte
- Webadressen von Repositories
- Dateinamen, Pfade der Dateien und Hash-Summen ausführbarer Dateien von Apps
- Namen der App-Kategorien

Protokollierung von Ereignissen im Protokoll des Betriebssystems konfigurieren

Standardmäßig werden Ereignisse, die während der Ausführung von Kaspersky Endpoint Security auftreten, nicht im Protokoll des Betriebssystems aufgezeichnet. Sie können die Aufzeichnung von Ereignissen in diesem Protokoll über die Web Console, die Verwaltungskonsole oder die Befehlszeile aktivieren.

In Kaspersky Security Center können Sie auch Ereignisse auswählen, die im Protokoll des Betriebssystems aufgezeichnet werden sollen.

Konfiguration in der Web Console

In der Web Console können Sie die Aufzeichnung von Ereignissen im Protokoll des Betriebssystems in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen** → **Allgemeine Einstellungen** → **App-Einstellungen**).

Wenn Sie im Abschnitt **Benachrichtigungen** auf den Link **Link Benachrichtigungen konfigurieren** klicken, wird das Fenster **Benachrichtigungen** geöffnet. In diesem Fenster können Sie mithilfe von Kontrollkästchen die Ereignisse auswählen, die von der App in Protokoll des Betriebssystems protokolliert werden soll.

Sie können einzelne Ereignistypen oder alle Ereignistypen einer bestimmten Wichtigkeitsstufe auswählen.

Standardmäßig sind alle Kontrollkästchen deaktiviert.

Konfiguration in der Verwaltungskonsole

In der Verwaltungskonsole können Sie die Aufzeichnung von Ereignissen im Protokoll des Betriebssystems in den Richtlinieneigenschaften konfigurieren (**Allgemeine Einstellungen** → **App-Einstellungen**).

Der Link **Konfigurieren** im Block **Benachrichtigungen** öffnet das Fenster **Benachrichtigungseinstellungen**. In diesem Fenster können Sie mithilfe von Kontrollkästchen die Ereignisse auswählen, die von der App in Protokoll des Betriebssystems protokolliert werden soll.

Sie können einzelne Ereignistypen oder alle Ereignistypen einer bestimmten Wichtigkeitsstufe auswählen.

Standardmäßig sind alle Kontrollkästchen deaktiviert.

Konfiguration über die Befehlszeile

Über die Befehlszeile können Sie die Aufzeichnung von Ereignissen im Protokoll des Betriebssystems mithilfe des Parameters `UseSyslog` in den allgemeinen App-Einstellungen aktivieren und deaktivieren.

Sie können den Wert des Parameters mithilfe von Befehlszeilenschaltern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen App-Einstellungen enthält.

Der Parameter `UseSyslog` kann die folgenden Werte annehmen:

- `Yes` – Protokollieren von Ereignissen im syslog aktivieren.
- `No` (Standardwert) – Protokollieren von Ereignissen im syslog deaktivieren.

Einstellungen des Ereignisprotokolls der App konfigurieren

Standardmäßig werden Informationen über Ereignisse im Ereignisprotokoll der App auf dem Gerät gespeichert. Über die Befehlszeile können Sie mithilfe der allgemeinen App-Einstellungen die folgenden Einstellungen für das Ereignisprotokoll der App konfigurieren:

- Ändern Sie den Pfad der Datenbank des Ereignisprotokolls der App mithilfe des Parameters `EventsStoragePath`. Standardwert: /var/opt/kaspersky/kesl/private/storage/events.db
- Legen Sie mithilfe des Parameters `MaxEventsNumber` die maximale Anzahl von Ereignissen fest, die die App speichern soll. Standardwert: 500000. Wenn die angegebene Anzahl von Ereignissen übertroffen wird, löscht die App die ältesten Ereignisse.

Sie können den Wert von Parametern mithilfe von Befehlszeilenschaltern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen App-Einstellungen enthält.

Ereignisse in Kaspersky Security Center anzeigen

Eine Liste aller Ereignisse während der Ausführung von Kaspersky Endpoint Security wird in der Web Console und in der Verwaltungskonsole angezeigt.

Sie können Benachrichtigungen über Ereignisse konfigurieren. Eine *Benachrichtigung* ist eine Nachricht mit Informationen über ein Ereignis, das auf einem geschützten Gerät aufgetreten ist. Mithilfe von Benachrichtigungen können Sie zeitnah über Ereignisse in der App informiert werden. Sie können die Ausführung eines Skripts beim Erhalt eines Ereignisses aus der App oder das Versenden von Ereignisbenachrichtigungen per E-Mail konfigurieren.

Nähere Informationen über die Verwendung von Ereignissen in Kaspersky Security Center finden Sie in der Hilfe zu Kaspersky Security Center.

Ereignisse über die Befehlszeile anzeigen

Über die Befehlszeile können Sie Folgendes anzeigen:

- aktuelle App-Ereignisse;
- Ereignisse aus dem Ereignisprotokoll der App.

Ausgabe aktueller Ereignisse

Sie können in der Konsole Informationen zu allen aktuellen App-Ereignissen oder zu aktuellen Ereignissen im Zusammenhang mit dem Starten oder Beenden einer bestimmten Aufgabe anzeigen. Über einen Filter können Sie sich auch bestimmte aktuelle Ereignisse anzeigen lassen, beispielsweise Ereignisse eines bestimmten Typs.

Um Informationen zu allen aktuellen App-Ereignissen in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control -W
```

Der Befehl gibt den Namen des Ereignisses und zusätzliche Informationen über das Ereignis zurück.

Um in die Konsole nur Informationen zu aktuellen Ereignissen, die mit der ausgeführten Aufgabe verknüpft sind, auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --start-task <ID/Name der Aufgabe> -W
```

Beispiel:
Ausgabe der aktuellen Ereignisse der gestarteten Aufgabe mit ID=1 aktivieren:

```
kesl-control --start-task 1 -W
```

Um Informationen zu aktuellen Ereignissen, die den Filterkriterien entsprechen, in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control -W --query "<Filterbedingungen>"
```

Filterbedingungen werden mithilfe eines oder mehrerer logischer Ausdrücke im Format `<Feld> <Vergleichsoperator> '<Wert>'` angegeben, die mit dem logischen Operator `and` kombiniert werden.

Beispiel:
Ausgeben der Ereignisse vom Typ "TaskStateChanged":

```
kesl-control -W --query "EventType == 'TaskStateChanged'"
```

Beispiel:
Ausgeben der Ereignisse vom Typ "TaskStateChanged", die vom Benutzer "User" angestoßen wurden.

```
kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'""
```

Ereignisse aus dem Ereignisprotokoll ausgeben

Sie können Informationen zu Ereignissen aus dem Ereignisprotokoll der App in die Konsole oder in eine Datei ausgeben. Sie können einen Filter verwenden, um bestimmte Ereignisse auszugeben.

Um Informationen zu allen Ereignissen im Ereignisprotokoll der App in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control -E --query [--db <Datenbankdatei>]
```

Wobei gilt:

- `<Datenbankdatei>` – Vollständiger Pfad zur Datenbankdatei des Ereignisprotokolls, aus dem Sie Ereignisse ausgeben möchten. Standardmäßig speichert die App die Informationen über Ereignisse in der Datenbank /var/opt/kaspersky/kesl/private/storage/events.db. Der Speicherort der Datenbank wird durch die allgemeine App-Einstellung `EventsStoragePath` bestimmt.

Mit dem Tool `less` können Sie durch die Liste der angezeigten Ereignisse navigieren. Standardmäßig speichert die App bis zu 500.000 Ereignisse. Die maximale Anzahl an Ereignissen, die von der Anwendung gespeichert werden, wird durch die allgemeine Einstellung der Anwendung namens `MaxEventsNumber` festgelegt.

Wenn sich das Ereignisprotokoll in der Standarddatenbank befindet, können Sie mit dem folgenden Befehl Informationen zu allen Ereignissen in die Konsole ausgeben:

```
kesl-control -E
```

Um Informationen zu Ereignissen im Ereignisprotokoll der App, die bestimmten Bedingungen entsprechen, in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control -E --query "<Filterbedingungen>" [--db <Datenbankdatei>] [-n <Anzahl>]
[--json] [--reverse]
```

Wobei gilt:

- `<Filterbedingungen>` – Ein oder mehrere logische Ausdrücke im Format `<Feld> <Vergleichsoperator> '<Wert>'`, kombiniert mit dem logischen Operator `and` zur Eingrenzung der Abfrageergebnisse.
- `<Anzahl>` – Anzahl der letzten Ereignisse aus der Auswahl (d. h. die Anzahl der Einträge ab Ende der Auswahl), die ausgegeben werden sollen.
- `--json` – Gibt die Ereignisse im JSON-Format aus.
- `--reverse` – Ereignisse in umgekehrter Reihenfolge anzeigen (das neueste Ereignis steht oben und das ältesten unten).

Um Informationen zu Ereignissen im Ereignisprotokoll der App, die bestimmten Bedingungen entsprechen, in eine Datei auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control -E --query "<Filterbedingungen>" [--db <Datenbankdatei>] [-n <Anzahl>] --file <Dateiname und Dateipfad> [--json]
```

Wobei gilt: `--file <Dateiname und Dateipfad>` – Vollständiger Pfad zu der Datei, in die Sie die Ereignisse ausgeben möchten.

Integritätsprüfung der App-Komponenten

Kaspersky Endpoint Security enthält eine Vielzahl verschiedener binärer Module in Form von dynamisch verbundenen Bibliotheken, ausführbaren Dateien, Konfigurationsdateien und Dateien der Oberfläche. Angreifer können ein oder mehrere ausführbare Module oder Dateien der App durch andere Dateien ersetzen, die bösartigen Code enthalten. Um einen solchen Austausch von Modulen und Dateien zu verhindern, bietet Kaspersky Endpoint Security die Funktion zur Integritätsprüfung der App-Komponenten. Die App überprüft Module und Dateien auf nicht autorisierte Änderungen und Schäden. Ein Modul oder eine Datei von der App mit einer nicht korrekten Prüfsumme gilt als beschädigt.

Eine Integritätsprüfung wird für die folgenden App-Komponenten durchgeführt, sofern diese auf dem Gerät installiert sind:

- das App-Paket
- das Paket der grafischen Benutzeroberfläche
- das Paket des Kaspersky Security Center Administrationsagenten
- das Verwaltungs-Plug-in für Kaspersky Endpoint Security

Die App überprüft die Integrität der Dateien, die in gesonderten Listen aufgeführt sind und *Manifestdateien* genannt werden. Jede App-Komponente verfügt über ihre eigene Manifestdatei, die eine Liste von App-Dateien enthält, deren Integrität für den korrekten Betrieb dieser App-Komponente wichtig ist. Der Name der Manifestdatei ist für jede Komponente gleich, der Inhalt der Manifestdateien ist jedoch unterschiedlich. Die Manifestdateien werden digital signiert. Auch ihre Integrität wird überprüft.

Die Integritätsprüfung der App-Komponenten erfolgt mit dem Tool zur Integritätsprüfung.

Die Integritätsprüfung muss unter einem Konto mit Root-Rechten ausgeführt werden.

Zur Integritätsprüfung können Sie sowohl das mit der App installierte Tool nutzen als auch ein Tool, das sich auf einer zertifizierten CD befindet.

Es wird empfohlen, das Tool zur Integritätsprüfung von einer zertifizierten CD zu starten, um die Integrität des Tools sicherzustellen. Wenn Sie das Tool von der CD ausführen, müssen Sie den vollständigen Pfad zur Manifestdatei angeben.

Das mit der App installierte Tool zur Integritätsprüfung befindet sich unter den folgenden Pfaden:

- zur Überprüfung des App-Pakets, des Pakets der grafischen Benutzeroberfläche und des Administrationsagenten: /opt/kaspersky/kesl/bin/integrity_checker
- zur Überprüfung des Verwaltungs-Plug-ins für Kaspersky Endpoint Security: im Verzeichnis mit den ausführbaren Modulen (DLLs) des Verwaltungs-Plug-ins:
  - Für 32-Bit-Betriebssysteme: %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<Version des Plugins>.plg\integrity_checker.exe
  - Für 64-Bit-Betriebssysteme: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<Version des Plugins>.plg\integrity_checker.exe

Die Manifestdateien finden Sie unter den folgenden Pfaden:

- /opt/kaspersky/kesl/bin/integrity_check.xml – zur Integritätsprüfung des App-Pakets
- /opt/kaspersky/kesl/bin/gui_integrity_check.xml – zur Integritätsprüfung des Pakets der grafischen Benutzeroberfläche
- /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml – zur Überprüfung des Administrationsagenten für 32-Bit-Betriebssysteme
- /opt/kaspersky/klnagent64/bin/kl_file_integrity_manifest.xml – zur Überprüfung des Administrationsagenten für 64-Bit-Betriebssysteme

Führen Sie den folgenden Befehl aus, um die Integrität von App-Komponenten zu überprüfen:

- So überprüfen Sie das App-Paket und das Paket für die grafische Benutzeroberfläche:

  `integrity_checker [<Pfad zur Manifestdatei>] --signature-type kds-with-filename`

- So überprüfen Sie das Verwaltungs-Plug-in von Kaspersky Endpoint Security und den Administrationsagenten:

  `integrity_checker [<Pfad zur Manifestdatei>]`

  Standardmäßig wird der Pfad zum Manifest verwendet, die sich in dem Verzeichnis befindet, in dem das Tool zur Integritätsprüfung ausgeführt wird.

Das Tool kann mit den folgenden optionalen Einstellungen ausgeführt werden:

- `--crl <Verzeichnis>` – Pfad des Verzeichnisses mit der Liste der widerrufenen Zertifikate (Zertifikatssperrliste).
- `--version` – Zeigt die Version des Tools an.
- `--verbose` – Ausführliche Ausgabe der durchgeführten Aktionen und Ergebnisse. Wenn Sie diese Einstellung nicht angeben, werden nur Fehler, Objekte, welche die Prüfung nicht bestanden haben, und die Gesamtstatistik der Untersuchung angezeigt.
- `--trace <Dateiname>`, wobei `<Dateiname>` der Name der Datei ist, in der Ereignisse mit der Informationstiefe DEBUG aufgezeichnet werden, die während der Untersuchung aufgetreten sind.
- `--signature-type kds-with-filename` – Typ der zu prüfenden Signatur (dieser Parameter ist obligatorisch für die Überprüfung des App-Pakets, des Pakets für die grafische Benutzeroberfläche und des Administrationsagenten).
- `--single-file <Datei>` – Überprüft nur eine im Manifest enthaltene Datei – die restlichen Manifest-Objekte werden ignoriert.

Eine Beschreibung aller verfügbaren Einstellungen des Tools zur Integritätsprüfung finden Sie in der Hilfe zu den Einstellungen des Tools, die Sie mithilfe des Befehls `integrity_checker --help` aufrufen.

Das Ergebnis der Überprüfung der Manifestdatei wird wie folgt angezeigt:

- `SUCCEEDED` – Die Integrität der Dateien wurde bestätigt (Rückgabecode 0).
- `FAILED` – Die Integrität der Dateien konnte nicht bestätigt werden (Rückgabecode ist nicht 0).

Wenn bei Starten der App ermittelt wird, dass die Integrität der App oder des Administrationsagenten verletzt ist, erstellt Kaspersky Endpoint Security das Ereignis *IntegrityCheckFailed* im Ereignisprotokoll und in Kaspersky Security Center.

App über die grafische Benutzeroberfläche verwalten

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, wird die grafische Benutzeroberfläche nicht unterstützt.

Mit der grafischen Benutzeroberfläche von Kaspersky Endpoint Security können Sie Folgendes tun:

- Informationen zum Schutzstatus des Geräts anzeigen.
- App-Komponenten aktivieren oder deaktivieren:
  - Schutz vor bedrohlichen Dateien.
  - Untersuchung von Wechseldatenträgern.
  - Schutz vor Web-Bedrohungen.
  - Schutz vor Netzwerkbedrohungen.
  - Schutz vor Verschlüsselung.
  - Firewall-Verwaltung.
  - App-Kontrolle.
  - Gerätekontrolle.
  - Verhaltensanalyse.
  - Überwachung der System-Integrität.
- Untersuchungsaufgaben starten und beenden:
  - Schadsoftware-Untersuchung.
  - Untersuchung wichtiger Bereiche.
  - Untersuchung von Containern.
- Datenbank-Update- und Rollback-Aufgaben starten und beenden.
- Benutzerdefinierte Untersuchung von Dateien und Verzeichnissen starten (wird gestartet, indem Sie mit der Maus auf eine Datei oder ein Verzeichnis klicken, das Sie untersuchen möchten).
- Die Verwendung von Kaspersky Security Network aktivieren und deaktivieren.
- Ausführungsstatistik der App und Berichte anzeigen.
- Lizenzschlüssel der App verwalten und Informationen zur Lizenz, unter der die App verwendet wird, und zu dem mit der Lizenz verknüpften Schlüssel anzeigen.
- Informationen zu Objekten anzeigen, die im Backup abgelegt wurden.
- Protokolldateien der App erstellen.

Wenn Komponente und Aufgabe der App im informativen Modus ausgeführt wird, zeigt die grafische Benutzeroberfläche der App für die Komponente und Aufgabe die Warnung *Informativer Ausführungsmodus ausgewählt* an.

Grafische Benutzeroberfläche

App-Symbol im Infobereich

Nach der Installation des Pakets der grafischen Benutzeroberflächen von Kaspersky Endpoint Security auf dem Gerät erscheint das App-Symbol im Infobereich der Taskleiste auf der rechten Seite.

Das App-Symbol fungiert als Verknüpfung zum Kontextmenü und zum Hauptfenster der App.

Das Kontextmenü der App enthält die folgenden Punkte:

- **Kaspersky Endpoint Security 12.1 für Linux**. Öffnet das Hauptfenster der App. Dieses Fenster zeigt den Schutzstatus Ihres Geräts an und enthält Elemente der Benutzeroberfläche, die den Zugriff auf die Funktionen der App ermöglichen.
- **Beenden**. Beendet die grafische Benutzeroberfläche der App.

Hauptfenster der App

Das Hauptfenster der App können Sie auf eine der folgenden Arten öffnen:

- Klicken Sie mit der rechten Maustaste oder doppelklicken Sie auf das App-Symbol im Infobereich der Taskleiste.
- Wählen Sie den App-Namen im Menü des Fenstermanagers des Betriebssystems.

Das Hauptfenster der App ist in mehrere Bereiche unterteilt:

- Der mittlere Bereich des Hauptfensters der App zeigt den Schutzstatus des Geräts. Durch einen Mausklick in diesen Fensterbereich gelangen Sie zum Fenster **Schutz-Center**. In diesem Fenster werden Informationen zum Schutzstatus des Geräts sowie Empfehlungen zu Maßnahmen angezeigt, die Sie gegebenenfalls zur Behebung von Problemen im Schutz ergreifen müssen.
- Die Schaltfläche **Untersuchung** zeigt den Status der Aufgabe zur Schadsoftware-Untersuchung und die Anzahl der gefundenen Bedrohungen an. Diese Schaltfläche öffnet das Fenster **Untersuchung**. In diesem Fenster können Sie die Aufgaben *Schadsoftware-Untersuchung*, *Untersuchung wichtiger Bereiche* und *Untersuchung von Containern* starten und beenden. Außerdem können Sie Berichte zu diesen Aufgaben anzeigen.
- Die Schaltfläche **Update** zeigt den Status der *Update-Aufgabe*. Diese Schaltfläche öffnet das Fenster **Update**. In diesem Fenster können Sie die *Update*-Aufgabe und das *Rollback des Datenbanken-Updates* starten. Außerdem können Sie Berichte zu diesen Aufgaben anzeigen.
- Der untere Bereich des Hauptfensters der App enthält die folgenden Elemente:
  - Die Schaltfläche **Berichte**. Diese Schaltfläche öffnet das Fenster **Berichte**, in dem Sie die Ausführungsstatistik der Komponenten und Aufgaben sowie diverse Berichte anzeigen können.
  - Die Schaltfläche **Backup**. Durch Anklicken dieser Schaltfläche wird das Fenster **Backup** geöffnet, das Informationen zu Objekten im Backup enthält.

- Die Schaltfläche **Einstellungen**. Diese Schaltfläche öffnet das Fenster **Einstellungen**, in dem Sie die Komponenten der App und die Verwendung von Kaspersky Security Network aktivieren und deaktivieren können.

- Die Schaltfläche **Support**. Durch Klicken auf diese Schaltfläche wird das Fenster **Support** geöffnet, in dem die aktuelle Version der App und die folgenden Informationen angezeigt werden:

  - **Schlüssel** – Aktiver Lizenzschlüssel, welcher der App hinzugefügt wurde, oder Information über das Fehlen eines Schlüssels. Über den Link in diesem Feld können Sie das Fenster **Lizenz** öffnen, in dem detaillierte Informationen zur Lizenz angezeigt werden.

  - **Schlüsselstatus** – Informationen über den Status des aktiven Lizenzschlüssels oder über das Fehlen eines aktiven Schlüssels.

  - **Veröffentlichungsdatum der Datenbank** – Status und Veröffentlichungsdatum der App-Datenbanken.

  - **Betriebssystem** – Informationen über das Betriebssystem des Geräts.

  Im linken unteren Bereich des Fensters wird neben Links, die zu den Informationsressourcen von Kaspersky führen, ein Link angezeigt, der das Fenster **Protokollierung** öffnet. In diesem Fenster können Sie Protokolldateien der App erstellen und den Detaillierungsgrad der Protokolldateien konfigurieren.

- Im unteren Teil des Hauptfensters der App werden Informationen zur Lizenz und zum Schlüssel sowie zu etwaigen Problemen mit der Lizenz angezeigt. Durch Klicken auf diesen Bereich des Fensters wird Fenster **Lizenz** geöffnet, in dem detaillierte Informationen zur Lizenz angezeigt werden.

  Wenn Sie in diesem Fenster auf die Schaltfläche **Lizenz erwerben** klicken, wird die Website des Kaspersky-Onlineshops geöffnet, auf der Sie eine Lizenz erwerben können. Nach dem Erwerb einer Lizenz erhalten Sie einen Aktivierungscode oder eine Schlüsseldatei, mit der Sie die App aktivieren müssen.

App-Komponenten aktivieren und deaktivieren

Über die grafische Benutzeroberfläche können Sie App-Komponenten aktivieren und deaktivieren. Wenn eine Komponente aktiviert ist, wird die Schaltfläche **Deaktivieren** verfügbar. Standardmäßig sind nur die Komponenten zum Schutz vor bedrohlichen Dateien, zur Gerätekontrolle und zur Verhaltensanalyse aktiviert. Die Komponente zum Schutz vor Web-Bedrohungen kann automatisch aktiviert werden, wenn auf dem Gerät die lokale Konfiguration des Schutzes vor Web-Bedrohungen aktiviert ist (d. h. es wird keine Richtlinie angewendet oder die Richtlinieneinstellungen werden nicht durch das "Schloss" gesperrt) und auf dem System einer der unterstützten Browser erkannt wird.

Wenn eine Komponente deaktiviert ist, wird die Schaltfläche **Aktivieren** verfügbar.

So aktivieren oder deaktivieren Sie eine App-Komponente:

1. Öffnen Sie das Hauptfenster der App.
2. Klicken Sie im unteren Bereich des Hauptfensters der App auf die Schaltfläche **Einstellungen**.

   Das Fenster **Einstellungen** wird geöffnet.
3. Klicken Sie für die gewünschte Komponente auf die Schaltfläche **Aktivieren** oder **Deaktivieren**.

Untersuchungsaufgaben starten und beenden

So starten oder stoppen Sie eine Untersuchungsaufgabe:

1. Öffnen Sie das Hauptfenster der App.
2. Klicken Sie im Hauptfenster der App auf die Schaltfläche **Untersuchung**.

   Das Fenster **Untersuchung** wird geöffnet.
3. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie eine Untersuchungsaufgabe starten möchten, klicken Sie auf die Schaltfläche **Starten** unterhalb der entsprechenden Untersuchungsaufgabe.

     Der Fortschritt der laufenden Untersuchungsaufgabe wird angezeigt.

   - Wenn Sie eine Untersuchungsaufgabe anhalten möchten, klicken Sie auf die Schaltfläche **Halt** unterhalb der entsprechenden Untersuchungsaufgabe.

     Die Untersuchungsaufgabe wird angehalten und es werden Informationen zu untersuchten Objekten und erkannten Bedrohungen angezeigt.
4. Wenn Sie einen Bericht über die Untersuchungsaufgabe möchten, klicken Sie auf die Schaltfläche **Bericht anzeigen**.

Wenn ein infiziertes Objekt erkannt wird oder die Untersuchungsaufgabe abgeschlossen ist, wird im Infobereich neben dem App-Symbol auf der rechten Seite der Taskleiste ein Pop-up-Fenster angezeigt.

Das Fenster **Untersuchung** zeigt auch den Fortschritt und die Ergebnisse temporärer Aufgaben zur Untersuchung von Bootsektoren (*Scan_Boot_Sectors_{ID}*) und temporärer Aufgaben zur benutzerdefinierten Untersuchung von Dateien (*Scan_File_{ID}*). Sie können die Informationen zu ausgeführten temporären Aufgaben ausblenden, indem Sie auf das Kreuzchen klicken oder das Fenster **Untersuchung** schließen (beim Wechsel zum Hauptfenster oder beim Verlassen der App).

Update-Aufgabe starten und beenden

So starten oder stoppen Sie eine Update-Aufgabe:

1. Öffnen Sie das Hauptfenster der App.
2. Klicken Sie im Hauptfenster der App auf die Schaltfläche **Update**.

   Das Fenster **Update** wird geöffnet.
3. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie eine Aufgabe starten möchten, klicken Sie auf die Schaltfläche **Starten** unterhalb der entsprechenden Aufgabe.

     Der Fortschritt der laufenden Update-Aufgabe wird angezeigt.

     Wenn die Update-Aufgabe erfolgreich abgeschlossen wurde, wird der Link **Update-Rollback** verfügbar und Sie können ein Rollback des letzten erfolgreichen Datenbanken-Updates durchführen.

   - Wenn Sie eine Aufgabe beenden möchten, klicken Sie auf **Halt** unterhalb der entsprechenden Aufgabe.

     Die Update-Aufgabe wird angehalten.
4. Wenn Sie einen Bericht über die Aufgabe anzeigen möchten, klicken Sie auf die Schaltfläche **Bericht anzeigen**.

So starten Sie eine Aufgabe zum Rollback des Updates:

1. Öffnen Sie das Hauptfenster der App.
2. Klicken Sie im Hauptfenster der App auf den Abschnitt **Update**.

   Das Fenster **Update** wird geöffnet.
3. Starten Sie die Aufgabe zum Rollback des Datenbanken-Updates, indem Sie auf den Link **Update-Rollback** klicken.

Verwendung von Kaspersky Security Network konfigurieren

Über die grafische Benutzeroberfläche können Sie die Verwendung von Kaspersky Security Network aktivieren und deaktivieren.

So aktivieren Sie die Verwendung von Kaspersky Security Network:

1. Öffnen Sie das Hauptfenster der App.
2. Klicken Sie im unteren Bereich des Hauptfensters der App auf die Schaltfläche **Einstellungen**.

   Das Fenster **Einstellungen** wird geöffnet.
3. Wählen Sie im Fenster **Einstellungen** eine der folgenden Optionen aus:

   - **Erweiterter KSN-Modus**, wenn Sie Kaspersky Security Network nutzen möchten, um Informationen aus der Wissensdatenbank abzurufen und anonyme Statistikdaten und Informationen über die Typen und Quellen der Bedrohungen zu senden.
   - **Standardmäßiger KSN-Modus**, wenn Sie Kaspersky Security Network nutzen möchten, um Informationen aus der Wissensdatenbank abzurufen, aber keine anonymen Statistikdaten und Informationen über die Typen und Quellen der Bedrohungen zu senden.
4. Klicken Sie auf die Schaltfläche **Aktivieren**.

   Das Fenster **Verwendung von Kaspersky Security Network**.
5. Lesen Sie im Fenster **Verwendung von Kaspersky Security Network** die Erklärung zu Kaspersky Security Network sorgfältig durch und wählen Sie die Option **Ich bestätige, dass ich die Bestimmungen und Bedingungen dieser Erklärung zu Kaspersky Security Network vollständig gelesen habe und sie verstehe und akzeptiere.**
6. Klicken Sie auf **OK**.

   Die Schaltfläche **OK** ist nicht verfügbar, wenn im Fenster **Verwendung von Kaspersky Security Network** keine der Optionen ausgewählt ist.

So deaktivieren Sie die Verwendung von Kaspersky Security Network:

1. Öffnen Sie das Hauptfenster der App.
2. Klicken Sie im unteren Bereich des Hauptfensters der App auf die Schaltfläche **Einstellungen**.

   Das Fenster **Einstellungen** wird geöffnet.
3. Klicken Sie auf die Schaltfläche **Deaktiviert**.
4. Klicken Sie im geöffneten Fenster auf **Ja**, um auf die Teilnahme an Kaspersky Security Network zu verzichten.

Berichte anzeigen

Über die grafische Benutzeroberfläche können Sie die Berichte der App anzeigen. Berichte zeichnen Informationen über die Ausführung der Komponenten und Aufgaben der App auf.

Die Berichtdaten werden als Tabelle angezeigt, die eine Liste von Ereignissen enthält. Jede Zeile der Tabelle enthält Informationen zu einem bestimmten Ereignis. Die Ereignisattribute werden in den Tabellenspalten angezeigt. Ereignisse, die während der Ausführung verschiedener Komponenten und Aufgaben protokolliert werden, haben unterschiedliche Attribute.

Die Berichte enthalten folgende Ereigniskategorien:

- *Kritisch* – Das sind Ereignisse von kritischer Bedeutung, die Sie beachten müssen, da sie auf Probleme mit der App oder auf Schwachstellen beim Schutz Ihres Geräts hinweisen.
- *Hoch.*
- *Mittel.*
- *Niedrig.*
- *Informativ.*
- *Fehler.*

Berichte werden in einem Fenster angezeigt, das durch Klicken auf die Schaltfläche **Berichte** unten im Hauptfenster der App geöffnet wird.

Die folgenden Berichte sind in der App verfügbar:

- **Statistik**. Dieser Bericht enthält statistische Daten zur Ausführung der Komponente "Schutz vor bedrohlichen Dateien" und den Untersuchungsaufgaben. Durch Klicken auf **Neu laden** können Sie den angezeigten Bericht aktualisieren.
- **Systemaudit**. Dieser Bericht enthält Informationen über Ereignisse, die bei der Ausführung der App und während der Interaktion des Benutzers mit der App auftreten.
- **Schutz vor Bedrohungen**. Dieser Bericht enthält Informationen über Ereignisse, die während der Ausführung der folgenden Komponenten der App protokolliert werden:
  - Schutz vor bedrohlichen Dateien.
  - Untersuchung von Wechseldatenträgern.
  - Schutz vor Verschlüsselung.
  - Schutz vor Web-Bedrohungen.
  - Schutz vor Netzwerkbedrohungen.
  - Firewall-Verwaltung.
  - App-Kontrolle.

- Gerätekontrolle.
- Verhaltensanalyse.
- Überwachung der System-Integrität.

- **Aufgaben auf Befehl**. Dieser Bericht enthält Informationen zu Ereignissen, die während der Ausführung von Untersuchungsaufgaben, Update-Aufgaben und Prüfungen der Systemintegrität protokolliert werden.

So zeigen Sie einen Bericht an:

1. Öffnen Sie das Hauptfenster der App.
2. Klicken Sie im unteren Bereich des Hauptfensters der App auf die Schaltfläche **Berichte**.

   Das Fenster **Berichte** wird geöffnet.
3. Wählen Sie im linken Bereich des Fensters **Berichte** den gewünschten Berichtstyp aus.

   Im rechten Bereich des Fensters wird der Bericht mit einer Liste von Ereignissen angezeigt.

   Standardmäßig werden die Ereignisse in aufsteigender Reihenfolge der Werte in der Spalte **Datum** sortiert.
4. Wenn Sie ausführliche Informationen über ein Ereignis anzeigen möchten, wählen Sie das entsprechende Ereignis im Bericht aus.

   Am unteren Rand des Fensters wird ein Block angezeigt, der die Attribute dieses Ereignisses enthält.

Für eine zweckmäßige Verarbeitung von Berichten können Sie die auf dem Bildschirm gezeigten Daten folgendermaßen ändern:

- Filtern Sie die Liste der Ereignisse nach dem Zeitpunkt ihres Auftretens.
- Suchen Sie mithilfe der Suchfunktion nach einem bestimmten Ereignis.
- Zeigen Sie das ausgewählte Ereignis in einem separaten Abschnitt an.

Objekte im Backup anzeigen

Über die grafische Benutzeroberfläche können Sie die folgenden Aktionen mit Backup-Objekten ausführen:

- Informationen zu Objekten anzeigen, die im Backup auf dem Gerät abgelegt wurden.
- Objekte aus dem Backup in ihren ursprünglichen Verzeichnissen wiederherstellen.
- Objekte aus dem Backup löschen. Entfernte Objekte können später nicht wiederhergestellt werden.

Informationen über die Wiederherstellung und Löschung von Objekten im Ereignisprotokoll aufzeichnen.

So zeigen Sie die Objekte im Backup an:

1. Öffnen Sie das Hauptfenster der App.
2. Klicken Sie im unteren Bereich des Hauptfensters der App auf die Schaltfläche **Backup**.

   Das Fenster **Backup** wird geöffnet.

Im Fenster werden folgende Informationen zu den Objekten im Backup angezeigt:

- Name des Objekts
- Vollständiger Pfad zum Objekt
- Datum, an dem das Objekt in das Backup verschoben wurde
- Datum, an dem das Objekt aus dem Backup gelöscht wurde (dieses Feld wird angezeigt, wenn eine Begrenzung der Speicherzeit von Objekten im Backup festgelegt ist)
- Objektgröße

Lizenzschlüssel verwalten

Über die grafische Benutzeroberfläche können Sie Lizenzschlüssel der App hinzufügen und entfernen sowie neben Informationen über die Lizenz, unter der die App verwendet wird, auch Informationen über die mit der Lizenz verknüpften Schlüssel anzeigen.

Sie können die App aktivieren, indem Sie einen aktiven Lizenzschlüssel hinzufügen.

Aktivierung – Vorgang, bei dem die App durch eine Lizenz aktiviert wird, die die Nutzung der Vollversion der App während der Gültigkeitsdauer der Lizenz ermöglicht.

Wenn Sie die App unter einer Lizenz verwenden, welche die Funktionalität von Kaspersky Endpoint Detection and Response Optimum nicht abdeckt, müssen Sie zur Aktivierung dieser Funktionalität einen zusätzlichen Lizenzschlüssel für das Add-on von Kaspersky Endpoint Detection and Response Optimum hinzufügen (im Weiteren auch "EDR Optimum-Schlüssel").

Sie können der App auch einen Reserveschlüssel hinzufügen. Der Reserveschlüssel wird aktiv, sobald die an den aktiven Schlüssel gebundene gültige Lizenz abläuft oder der aktive Schlüssel gelöscht wird. Ein Reserveschlüssel verhindert, dass nach Ablauf der Lizenz die Funktionalität der App eingeschränkt wird.

Ein Reserveschlüssel kann nur hinzugefügt werden, wenn bereits ein aktiver Lizenzschlüssel hinzugefügt wurde.

Einen Lizenzschlüssel hinzufügen

So fügen Sie der App einen aktiven Lizenzschlüssel hinzu:

1. Öffnen Sie das Hauptfenster der App.
2. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie im unteren Teil des Hauptfensters der App auf den Bereich des Fensters, in dem Informationen zur Lizenz und zum Schlüssel angezeigt werden.
   - Klicken Sie im unteren Teil des Hauptfensters der App auf die Schaltfläche **Support** und öffnen Sie im geöffneten Fenster **Support** das Fenster **Lizenz** über den Link im Feld **Schlüssel**.

Das Fenster **Lizenz** wird geöffnet. Wenn Sie in diesem Fenster auf die Schaltfläche **Lizenz erwerben** klicken, wird die Website des Kaspersky-Onlineshops geöffnet, auf der Sie eine Lizenz erwerben können.

3. Sie können die App sowohl mit einer kommerziellen Lizenz als auch mit einer Testlizenz aktivieren.

   So aktivieren Sie die App unter einer kommerziellen Lizenz:

   a. Klicken Sie im Block **Kommerzieller Schlüssel** auf die Schaltfläche **Hinzufügen** und führen Sie je nach Methode zum Hinzufügen des Schlüssels die folgenden Aktionen aus:

      - Wenn Sie einen Schlüssel mithilfe eines Aktivierungscodes hinzufügen möchten, geben Sie den Aktivierungscode ein und klicken Sie auf die Schaltfläche **Weiter**.
      - Wenn Sie einen Schlüssel mithilfe einer Schlüsseldatei hinzufügen möchten, klicken Sie auf die Schaltfläche **Schlüssel hinzufügen** und wählen Sie im sich öffnenden Fenster eine Datei mit key-Erweiterung aus.

      Das Fenster zeigt Informationen über den Schlüssel und die mit ihm verbundene Lizenz an.

   b. Klicken Sie auf **Aktivieren**.

   Um die App mit einer Testlizenz zu aktivieren, klicken Sie im Block **Testschlüssel** auf die Schaltfläche **Aktivieren**. Das Fenster zeigt Informationen über die Testlizenz und den zugehörigen Schlüssel an.

   > Sie können die App im Rahmen einer Testlizenz nur einmal für einen Testzeitraum verwenden.

Nach dem Hinzufügen des aktiven Anwendungsschlüssels können Sie einen Backup-Schlüssel und bei Bedarf einen zusätzlichen EDR Optimum-Schlüssel hinzufügen. Um den Vorgang zum Hinzufügen eines Reserveschlüssels oder eines zusätzlichen Schlüssels zu beginnen, verwenden Sie die Schaltfläche **Hinzufügen** im oberen Bereich des Fensters **Lizenz**.

Einen Lizenzschlüssels entfernen

So entfernen Sie zur App hinzugefügten einen Lizenzschlüssel:

1. Öffnen Sie das Hauptfenster der App.
2. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie im unteren Teil des Hauptfensters der App auf den Bereich des Fensters, in dem Informationen zur Lizenz und zum Schlüssel angezeigt werden.
   - Klicken Sie im unteren Teil des Hauptfensters der App auf die Schaltfläche **Support** und öffnen Sie im geöffneten Fenster **Support** das Fenster **Lizenz** über den Link im Feld **Schlüssel**.

   Das Fenster **Lizenz** wird geöffnet.

3. Klicken Sie rechts neben Informationen zu dem Schlüssel, den Sie löschen möchten, auf die Schaltfläche **Löschen**.
4. Bestätigen Sie den Löschvorgang im sich öffnenden Fenster.

Informationen zur Lizenz anzeigen

So zeigen Sie Informationen zur Lizenz an:

1. Öffnen Sie das Hauptfenster der App.
2. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie im unteren Teil des Hauptfensters der App auf den Bereich des Fensters, in dem Informationen zur Lizenz und zum Schlüssel angezeigt werden.
   - Klicken Sie im unteren Teil des Hauptfensters der App auf die Schaltfläche **Support** und öffnen Sie im geöffneten Fenster **Support** das Fenster **Lizenz** über den Link im Feld **Schlüssel**.

   Das Fenster **Lizenz** wird geöffnet.

Das Fenster zeigt Informationen über die Lizenz an, unter der die App verwendet wird. Wenn der App ein Reserveschlüssel hinzugefügt wurde, werden auch die Informationen über die Lizenz angezeigt, die mit dem Reserveschlüssel verknüpft ist. Klicken Sie auf **Mehr darüber**, um die vollständigen Informationen zu den Lizenzen und Schlüsseln anzuzeigen.

Im Block **Aktive Lizenzen** werden folgende Informationen zu den aktiven Schlüsseln und zu den mit ihnen verknüpften Lizenzen angezeigt:

- Typ der aktiven Lizenz der App, Lizenzbeschränkungen und Ablaufdatum der Lizenz.
- **Schlüssel** – Eindeutige Folge aus Buchstaben und Ziffern.
- **Schlüsselstatus** – Status des Schlüssels oder eine Benachrichtigung über etwaige Probleme mit dem Schlüssel.
- **Aktivierungsdatum** – Datum der Aktivierung der App durch Hinzufügen dieses Schlüssels.
- **Verbleibend** – Anzahl der Tage bis zum Ablauf der Lizenz und Ablaufdatum der Lizenz im UTC-Format.
- **Name der Anwendung** – Der Name der App, für deren Aktivierung der Schlüssel vorgesehen ist.
- **Schutz** – Informationen über Einschränkungen der Schutzfunktionen und über die Aktualisierung von App-Datenbanken.

Wenn Sie der App einen aktiven EDR Optimum-Schlüssel hinzugefügt haben, werden die Informationen zu diesem Schlüssel und der zugehörigen Lizenz ebenfalls im Block **Aktive Lizenzen** angezeigt.

Im Block **Reserveschlüssel** werden die folgenden Informationen zu den Reserveschlüsseln und ihren zugehörigen Lizenzen angezeigt:

- Typ des Reserveschlüssels, Lizenzbeschränkungen und Ablaufdatum der mit dem Schlüssel verknüpften Lizenz.
- **Schlüssel** – Eindeutige Folge aus Buchstaben und Ziffern.
- **Lizenztyp** – Typ der mit dem Sicherungsschlüssel verknüpften Lizenz.
- **Name der Anwendung** – Der Name der App, für deren Aktivierung der Schlüssel vorgesehen ist.

- **Schutz** – Informationen über Einschränkungen der Schutzfunktionen und über die Aktualisierung von App-Datenbanken.

Wenn Sie der App einen EDR Optimum-Reserveschlüssel hinzugefügt haben, werden die Informationen zu diesem Schlüssel und der zugehörigen Lizenz ebenfalls im Block **Reserveschlüssel** angezeigt.

Protokolldatei erstellen

Über die grafische Benutzeroberfläche können Sie Protokolldateien der App erstellen und den Detaillierungsgrad der Protokolldateien konfigurieren.

So erstellen Sie eine Protokolldatei:

1. Öffnen Sie das Hauptfenster der App.
2. Klicken Sie im unteren Bereich des Hauptfensters der App auf die Schaltfläche **Support**.

   Das Fenster **Support** wird geöffnet.
3. Klicken Sie auf den Link **Protokollierung**, um das Fenster **Protokollierung** zu öffnen.
4. Wählen Sie in der Dropdown-Liste Level die **Stufe** der Protokolldatei.

   Sie sollten sich bei der Festlegung der erforderlichen Informationstiefe an die Empfehlung der Experten des Technischen Supports von Kaspersky halten. Standardmäßig beträgt der Wert **Diagnose (300)**.
5. Klicken Sie auf die Schaltfläche **Aktivieren**, um den Protokollierungsvorgang zu starten.
6. Reproduzieren Sie die Situation, in der das Problem auftritt.
7. Klicken Sie auf die Schaltfläche **Deaktivieren**, um den Protokollierungsvorgang zu beenden.

Die erstellten Protokolldateien werden im Verzeichnis /var/log/kaspersky/kesl/ gespeichert.

Container-App Kaspersky Endpoint Security (KESL-Container)

Der Lieferumfang der App Kaspersky Endpoint Security enthält Dateien zum Erstellen einer Container-App (im Folgenden auch "KESL-Container"), die in externe Systeme integriert wird, um Container-Images in Image-Repositories zu untersuchen.

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, wird die Funktionalität für KESL-Container nicht unterstützt.

Mit dem KESL-Container können Sie Folgendes tun:

- Container-Images in Repositories untersuchen.
- Untersuchte Images, die keine infizierten Objekte enthalten, in ein vertrauenswürdiges Repository übermitteln.

Nach der Bereitstellung, Aktivierung und Konfiguration des KESL-Containers sind darin die folgenden Funktionskomponenten und Aufgaben von Kaspersky Endpoint Security verfügbar:

- Komponente "Schutz vor bedrohlichen Dateien".
- Untersuchungsaufgaben:
  - Schadsoftware-Untersuchung.
  - Untersuchung wichtiger Bereiche.
  - Container untersuchen.
- Komponente "Container-Überwachung".

Im KESL-Container stehen folgende Zusatzfunktionen von Kaspersky Endpoint Security zur Verfügung:

- Aktivierung der App mithilfe einer Schlüsseldatei oder eines Aktivierungscodes.
- Update der App-Datenbanken und Rollback des Datenbanken-Updates.
- Speicherung von Backup-Kopien von Dateien im Backup auf dem Gerät.

Die Interaktion mit dem KESL-Container erfolgt über die REST-API. Sie können die Einstellungen des KESL-Containers auch in Kaspersky Security Center mithilfe von Richtlinien konfigurieren.

Für den ordnungsgemäßen Betrieb von KESL-Containern wird empfohlen, in Kaspersky Security Center jene Geräte, die KESL-Containern entsprechen, in eine separate Administrationsgruppe mit eigener Richtlinie zu verschieben. In den Richtlinieneinstellungen können alle Funktionen und Einstellungen von Kaspersky Endpoint Security bearbeitet werden, die Konfiguration von Einstellungen, die im KESL-Container nicht unterstützt werden, hat jedoch keinen Einfluss auf den Betrieb des KESL-Containers.

Die Verwaltung des KESL-Containers über die Befehlszeile wird nicht unterstützt.

Wenn der KESL-Container während der Bereitstellung aktiviert und mit Kaspersky Security Center verbunden wurde und wenn in Kaspersky Security Center die automatische Verteilung des Lizenzschlüssels auf verwaltete Geräte konfiguriert ist, wird dieser Schlüssel nicht auf Geräte angewendet, die KESL-Containern entsprechen.

KESL-Container bereitstellen und aktivieren

Beschreibung des Programmpakets

Das Programmpaket enthält die folgenden Dateien:

- docker-service-<Version>.tgz – Archiv mit Dateien, die zur Image-Erstellung erforderlich sind.
- kesl-<Version>.rpm – Installationspaket für Kaspersky Endpoint Security.
- klnagent.rpm – Installationspaket des Kaspersky Security Center Administrationsagenten.

Das Archiv docker-service-<Version>.tgz enthält die folgenden Dateien:

- kesl-service – Verzeichnis mit den Dateien der Container-App.
- Dockerfile – Datei zum Erstellen eines Docker-Images mit einer Version unter 18.06.
- Dockerfile.1809 – Datei zum Erstellen eines Docker-Images mit einer Version höher als 18.05.
- build.sh.example – Beispielskript zum Erstellen eines Images.
- run.sh.example – Beispielskript zum Starten eines KESL-Containers.
- kesl-service.config.example – Beispiel für eine Konfigurationsdatei der Container-App.
- klnagent.conf.example – Beispiel für eine Konfigurationsdatei für die Verbindung zu Kaspersky Security Center.
- readme.md – Kurzhilfe.

KESL-Container bereitstellen und aktivieren

So bereiten Sie einen KESL-Container für die Verwendung vor:

1. Entpacken Sie das Archiv tar -xvf docker-service-<Version>.tgz.
2. Wenn Sie die Einstellungen des KESL-Containers über Kaspersky Security Center anpassen möchten, gehen Sie wie folgt vor:
   a. Geben Sie in der Datei klnagent.conf.example die Variablenwerte des Administrationsagenten an. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security Center (Abschnitt *Installation des Administrationsagenten für Linux im Silent-Modus (mit einer Antwort-Datei)*).
   b. Kopieren Sie klnagent.conf.example nach kesl-service/klnagent.conf.

3. Erstellen Sie das Docker-Image des KESL-Containers mit dem Installationsskript build.sh.example:

   a. Falls Sie einen Proxy-Server verwenden, geben Sie die gewünschten Werte für die Variable COMMON_AGRS an.

   b. Ersetzen Sie bei Bedarf den Namen des Ziel-Images "kesl-service" mit einem eigenen Namen.

   c. Kopieren Sie build.sh.example nach build.sh und geben Sie dem Skript das Attribut einer ausführbaren Datei.

   d. Führen Sie build.sh aus.

4. Stellen Sie sicher, dass die Erstellung erfolgreich war, indem Sie den Befehl `docker images -a` ausführen.

   Das folgende Ergebnis der Befehlsausführung wird angezeigt:

   ```
   REPOSITORY TAG IMAGE ID CREATED SIZE
   kesl-service latest <hex> < Zeitpunkt der Erstellung > < Größe >
   ```

5. Aktivieren Sie den KESL-Container auf eine der folgenden Arten:

   - über Kaspersky Security Center. Zur Aktivierung eines KESL-Containers müssen Sie den Schlüssel zu Geräten, die KESL-Containern entsprechen, in der Web Console oder in der Verwaltungskonsole hinzufügen.

     > Für den ordnungsgemäßen Betrieb von KESL-Containern wird empfohlen, in Kaspersky Security Center jene Geräte, die KESL-Containern entsprechen, in eine separate Administrationsgruppe mit eigener Richtlinie zu verschieben. Wenn der KESL-Container angehalten wird, werden diese Geräte automatisch aus der Administrationsgruppe entfernt und der auf diesen Geräten verwendete Schlüssel wird freigegeben.

   - mithilfe der Konfigurationsdatei.

   - mithilfe der Umgebungsvariablen (siehe Schritt 7).

6. Konfigurieren Sie den KESL-Container (KESL-Container konfigurieren, Einstellungen des KESL-Containers).

7. Starten Sie den KESL-Container mit dem Befehl `docker run --privileged --init -p < Port_des_KESL-Containers >:< Port_des_Geräts > \`

   ```
   -e < Variable_1 > -e < Variable_2 > ... -e < Variable_n > \
   -v < Mountpunkt_1 > -v < Mountpunkt_2 > ... -v < Mountpunkt_n > \
   < Image-Name >
   ```

   Wobei gilt:

   - `< Port_des_KESL-Containers >` – Port des KESL-Containers, der für das Netzwerk außerhalb des KESL-Containers verfügbar sein soll.

   - `< Port_des_Geräts >` – der Port des Gerätes, auf dem der KESL-Container installiert ist.

   Wenn Sie den KESL-Container starten, können Sie den KESL-Container über eine Umgebungsvariable aktivieren:

   - Wenn Sie einen Aktivierungscode verwenden, fügen Sie den Parameter `KRAS4D_ACTIVATION='< Aktivierungscode >'` hinzu:

     ```
     docker run ... -e KRAS4D_ACTIVATION='< Aktivierungscode >'
     ```

- Wenn Sie eine Schlüsseldatei verwenden, fügen Sie die Parameter `KRAS4D_ACTIVATION='<Schlüsseldatei>'` und `KRAS4D_KEYPATH=/root/kesl-service/keys` hinzu:

  ```
  docker run ... -e KRAS4D_ACTIVATION='<Schlüsseldatei>' -e
  KRAS4D_KEYPATH=/root/kesl-service/keys -v <Pfad zum
  Schlüsselverzeichnis>:/root/kesl-service/keys
  ```

Ein Beispiel für den Ausführungsbefehl finden Sie in der Datei "run.sh.example".

KESL-Container konfigurieren

Die Einstellungen des KESL-Containers können auf verschiedene Arten initialisiert werden:

- Standardmäßig (sofern nicht anders angegeben).
- Aus der Konfigurationsdatei. In diesem Fall haben die Werte aus der Konfigurationsdatei Vorrang vor den Standardwerten.
- Durch Übermittlung der Werte als Umgebungsvariablen an den KESL-Container bei seinem Start. Die Umgebungsvariablen haben Vorrang vor den Einstellungen der Konfigurationsdatei.
- Im Textkörper der Untersuchungsanforderung. die Einstellungen im Textkörper der Anforderung haben Vorrang vor allen anderen Werten, sind jedoch nur im Rahmen einer einzelnen Anforderung gültig.

Einstellungen des KESL-Containers

Die Einstellungen des KESL-Containers und ihre Standardwerte sind in der folgenden Tabelle aufgeführt.

Einstellungen des KESL-Containers

Beschreibung der Einstellung	Mögliche Werte
Port zum Abhören der REST API	
Ereigniskategorie	`debug` – für Debugging `info` – informativ `warning` – Warnung `error` – Fehler `critical` – kritisch `noset` – nicht angegeben
Autorisierungsschlüssel	Bei Angabe der Einstellung `KRAS4D_XAPIKEY` wird für jede Anforderung geprüft, ob der Header "x-api-key" vorhanden ist und ob sein Inhalt mit dem Wert der Einstellung `KRAS4D_XAPIKEY` übereinstimmt. Wenn diese Bedingungen nicht erfüllt sind, wird die Anforderung abgelehnt. Fehlt diese Einstellung, wird die Überprüfung nicht durchgeführt.
Aktivierungscode oder Schlüsseldatei	Zur Aktivierung eines KESL-Containers mithilfe eines Aktivierungscodes müssen Sie beim Start des KESL-Containers den Aktivierungscode in der Konfigurationsdatei angeben oder ihn mithilfe einer Umgebungsvariablen übergeben:

	`docker run ... -e KRAS4D_ACTIVATION='<Aktivierungscode>'`
	Zur Aktivierung eines KESL-Containers mithilfe einer Schlüsseldatei müssen Sie beim Start des KESL-Containers die Schlüsseldatei in der Konfigurationsdatei angeben oder sie mithilfe einer Umgebungsvariablen übergeben:
	`docker run ... -e KRAS4D_ACTIVATION='<Schlüsseldatei>' -e KRAS4D_KEYPATH=/root/kesl-service/keys -v <Pfad zum Schlüsselverzeichnis>:/root/kesl-service/keys`
	Zur Aktivierung eines KESL-Containers mithilfe einer Schlüsseldatei ist der Mountpunkt /root/kesl-service/keys erforderlich.

Zusätzliche Untersuchungseinstellungen	Mit der optionalen Einstellung `KRAS4D_SCANOPTIONS` können Sie die Einstellungen der Aufgabe zur Untersuchung von Containern konfigurieren: `docker run ... -e KRAS4D_SCANOPTIONS='<Einstellungen>'` wobei `<Einstellungen>` die Einstellungen der Aufgabe "Untersuchung von Containern" sind.
Zusätzliche Update-Einstellungen	Mit der optionalen Einstellung `KRAS4D_UPDATEOPTIONS` können Sie die Einstellungen der Update-Aufgabe konfigurieren: `docker run ... -e KRAS4D_UPDATEOPTIONS='<Einstellungen>'` wobei `<Einstellungen>` die Einstellungen der Update-Aufgabe `SourceType`, `ApplicationUpdateMode` und die Einstellungen des Abschnitts `CustomSources.item_#` sind.
Apps-Datenbanken beim Start des KESL-Containers aktualisieren	Standardmäßig werden die App-Datenbanken beim Start des KESL-Containers in das Verzeichnis "/var/opt/kaspersky/kesl/private/updates" heruntergeladen. Um mehrere KESL-Container mit einer einzigen Instanz der App-Datenbanken zu betreiben und/oder den Start des KESL-Containers zu beschleunigen, wird empfohlen, dieses Verzeichnis durch Mounten auf das Gerät auszulagern, auf dem der KESL-Container installiert ist: `docker run ... -v <Pfad zum Datenbankverzeichnis>:/var/opt/kaspersky/kesl/private/updates`
Image nicht verarbeiten, wenn dieses sich bereits im Ziel-Repository befindet	
Maximale Wartezeit für die Ausführung der App-Befehle in Sekunden	
Maximale Wartezeit für die Ausführung der Aufgabe zum Aktualisieren der App-Datenbanken in Sekunden	
Name der Konfigurationsdatei des KESL-Containers	

Umgebungsvariablen

Zur Konfiguration des KESL-Containers sind die folgenden Umgebungsvariablen verfügbar:

- KRAS4D_PORT – Port zum Abhören der REST API.
- KRAS4D_LOGLEVEL – Ereigniskategorie.
- KRAS4D_XAPIKEY – Schlüssel für die Autorisierung der Anforderung.
- KRAS4D_ACTIVATION – Aktivierungscode oder Name der Schlüsseldatei.
- KRAS4D_SCANOPTIONS – Zusätzliche Untersuchungseinstellungen.
- KRAS4D_UPDATEOPTIONS – Zusätzliche Update-Einstellungen.
- KRAS4D_FORCEUPDATE – App-Datenbanken beim Start des KESL-Containers aktualisieren.
- KRAS4D_SKIPIMAGEIFEXISTS – Image nicht verarbeiten, wenn dieses sich bereits im Ziel-Repository befindet.
- KRAS4D_GENERALTIMEOUT – Maximale Wartezeit für die Ausführung der App-Befehle.
- KRAS4D_UPDTASKTIMEOUT – Maximale Wartezeit für die Ausführung der Aufgabe zum Aktualisieren der App-Datenbanken.
- KRAS4D_CFGNAME – Name der Konfigurationsdatei des KESL-Containers.

Konfigurationsdatei

Die Konfigurationsdatei des KESL-Containers liegt im yaml-Format vor. Um die Einstellungen aus der Datei lesen zu können, müssen Sie den Pfad /root/kesl-service/config/ auf dem Gerät mounten, auf dem der KESL-Container installiert ist, und den Namen der Konfigurationsdatei angeben, wenn dieser vom Standardnamen abweicht. Auf diese Weise können Sie für jeden Satz von KESL-Containern eine eigene Konfigurationsdatei angeben.

Beispiel für den Start eines KESL-Containers:

```
docker run ... \
-e KRAS4D_CFGNAME='eindeutiger_dateiname' \
-v <HOST_PATH>:/root/kesl-service/config \
kesl-service
```

Die folgende Tabelle enthält die Einstellungen der Konfigurationsdatei und die entsprechenden Umgebungsvariablen.

Einstellungen und zugehörige Umgebungsvariablen

Einstellung der Konfigurationsdatei	Umgebungsvariable
Abschnitt "common"	
port: <zu überwachender Port>	# KRAS4D_PORT=8085
sqlpath: <vollständiger Pfad zur Datenbankdatei mit den Untersuchungsergebnissen>	# KRAS4D_SQLPATH
certdir: <Pfad zum Verzeichnis mit Registrierungszertifikaten>	# KRAS4D_CERTDIR
keypath: <Pfad zum Verzeichnis mit Lizenzschlüsseln>	# KRAS4D_KEYPATH
tmppath: <vollständiger Pfad zum temporären Verzeichnis>	# KRAS4D_TMPPATH
logpath: <vollständiger Pfad zum Ereignisprotokoll>	# KRAS4D_LOGPATH

loglevel: [noset|debug|info|warning|error|critical]	# KRAS4D_LOGLEVEL
Abschnitt "control"	
xapikey: <Schlüssel für die Autorisierung der Anforderung>	# KRAS4D_XAPIKEY=None
forceupdate: <Datenbanken-Update bei Container-Start erzwingen [True|False]>	# KRAS4D_FORCEUPDATE
activation: <Aktivierungscode oder Name der Schlüsseldatei aus /root/kesl-service/config/>	# KRAS4D_ACTIVATION
detectaction: [delete|skip]	# KRAS4D_DETECTACTION
scanoptions: <Untersuchungseinstellungen [ScanArchived=yes ScanSfxArchived=yes ...]>	# KRAS4D_SCANOPTIONS
skipimageifexist: <Image nicht untersuchen, wenn es bereits auf dem Server vorhanden ist, auf den das untersuchte Image kopiert werden soll>	# KRAS4D_SKIPIMAGEIFEXIST
generaltimeout: <maximale Wartezeit für die Ausführung von App-Befehlen>	# KRAS4D_GENERALTIMEOUT
updtasktimeout: <maximale Wartezeit für die Ausführung der Aufgabe zum Aktualisieren der App-Datenbanken>	# KRAS4D_UPDTASKTIMEOUT
Abschnitt "repositories"	
<server>:<port>: Adresse und Port der Image-Registrierung, die bei einer Untersuchungsanforderung eine Autorisierung erfordert	
Unterabschnitt "credentials"	
user: Benutzername für die Autorisierung in der Image-Registrierung	
pass: Kennwort für die Autorisierung in der Image-Registrierung	

Beispiel einer Konfigurationsdatei:

```
common:
    port: 8085
    sqlpath: './data/scans.sqlite'
    tmppath: './tmp/'
    keypath: './keys/'
    certdir: './certificates/'
    logpath: '/var/log/kaspersky/kesl-service/'
    loglevel: 'debug'
control:
    xapikey: 0000
    activation: XXXX-XXXX-XXXX-XXXX or XXXX.key
    scanoptions: 'ScanArchives=yes'
    updateoptions: ''
    forceupdate: True
    skipimageifexists: False
    generaltimeout: 600
    updtasktimeout: 1000
repositories:
    repository.any.com:
        certificate: repository_any_comcert.pem
        credentials:
            user: user
            pass: password
```

Verfügbare Mountpunkte

Zur Verwendung des KESL-Containers stehen folgende Mountpunkte zur Verfügung:

- /root/kesl-service/data/scans.sqlite – Pfad zur Datenbankdatei mit den Untersuchungsergebnissen.
- /var/opt/kaspersky/kesl/private/updates – Pfad zu den App-Datenbanken.

- /root/kesl-service/certificates – Pfad zum Verzeichnis mit den Repository-Zertifikaten.
- /root/kesl-service/keys – Pfad zum Verzeichnis mit den Lizenzschlüsseln.
- /var/log/kaspersky/ – Pfad zum Verzeichnis mit den Ereignisprotokollen.
- /root/kesl-service/config/ – Pfad zu den Konfigurationsdateien.
- /var/lib/containers/vfs-storage – Obligatorischer Mountpunkt für den ordnungsgemäßen Betrieb des Podman-Tools.

Verwaltung von KESL-Containern über die REST API

Die Interaktion mit dem KESL-Container erfolgt über die REST API. Mit der REST-API können Sie Folgendes tun:

- Eine Datei oder mehrere Dateien untersuchen. Senden Sie dazu eine Untersuchungsanforderung (POST).

  Beispiel:
  POST http://<server>:<port>/scans

  Eine Datei oder mehrere Dateien.

- Ein Docker-Image oder mehrere Docker-Images untersuchen. Senden Sie dazu eine Untersuchungsanforderung (POST).

  Beispiel:
  POST http://<server>:<port>/scans

  Link zum Docker-Image oder zu den Docker-Images, die untersucht werden sollen.

- Ein Docker-Image oder mehrere Docker-Images mit zusätzlichen Einstellungen untersuchen. Senden Sie dazu eine Untersuchungsanforderung (POST).

  Beispiel:
  POST http://<server>:<port>/scans

  JSON einer bestimmten Art.

- Eine Liste mit Untersuchungssitzungen abrufen. Senden Sie dazu eine Anforderung zum Abruf von Informationen zu Untersuchungssitzungen (GET).

  Beispiel:
  GET http://<server>:<port>/scans

- Informationen zur Untersuchungssitzung abrufen. Senden Sie dazu eine Anforderung zum Abruf von Informationen zu Untersuchungssitzungen (GET).

  Beispiel:
  GET http://<server>:<port>/scans/<eindeutige ID der Untersuchungssitzung>

- Hinzufügen des Registrierungszertifikats ohne Neustart des KESL-Containers. Senden Sie dazu Anforderung zum Hinzufügen eines Registrierungszertifikats (POST).

  Beispiel:
  POST http://<server>:<port>/addcert

- Abrufen von Informationen über den Status des KESL-Containers. Senden Sie dazu eine Anfrage zum Abrufen von Informationen über den Status des KESL-Containers (GET).

  Beispiel:
  GET http://<Server>:<Port>/status

Untersuchungsanforderung (POST)

Ziel

Untersuchung des Objekts, das im Textkörper der Anforderung angegeben ist

Die Untersuchung ist für folgende Objekte vorgesehen:

- eine Datei
- mehrere Dateien
- Docker-Image oder mehrere Docker-Images in einem bestimmten Repository
- Docker-Image oder mehrere Docker-Images in einem bestimmten Repository mit Angabe zusätzlicher Einstellungen

Pfad

http://<server>:<port>/scans[?wait=1]

Einstellungen

Die optionale Einstellung `wait` gibt den Typ der Untersuchungssitzung an.

Wenn die Einstellung den Wert `1` besitzt, wird eine synchrone Untersuchung durchgeführt und die App versendet nach Beendigung der Untersuchung einen Bericht.

Wenn die Einstellung den Wert `0` besitzt, wird eine asynchrone Untersuchung durchgeführt und die Antwort sieht wie folgt aus:

```
{

  "id"="7d27e9b4-a4d7-469b-bdcf-ebfe953498e4",

  "location"="/scans/7d27e9b4-a4d7-469b-bdcf-ebfe953498e4"

}
```

Wobei gilt:

- id – Eindeutige ID der Untersuchungssitzung

- location – Pfad zur Anforderung von Informationen zu diesem Abschnitt vom Typ http://<server>:<port>/scans/<location>

Header der Anforderung

Die Anforderung kann die folgenden Header enthalten:

- Content-Type

  Definiert den Objekttyp, der zur Untersuchung übergeben wird.

  Unterstützte Werte:

  - application/octet-stream – eine Datei
  - multipart/form-data – mehrere Dateien
  - text/plain – Docker-Image oder mehrere Docker-Images in einem bestimmten Repository
  - application/json – Docker-Image oder mehrere Docker-Images in einem bestimmten Repository mit Angabe zusätzlicher Einstellungen

- x-api-key (optional)

  API-Schlüssel, wie in der Umgebungsvariablen KRAS4D_XAPIKEY oder der Variablen "xapikey" in der Konfigurationsdatei angegeben

Mögliche Fehler

Wenn im Header "Content-Type" ein nicht unterstützter Wert angegeben wird, gibt die App einen Fehler des folgenden Typs zurück:

```
{

  "error"={

"code"="NOT_SUPPORTED_CONTENT_TYPE",
"details"="<content type>",
"message"="Not supported Content-Type"

  },

  "status"="error"

}
```

Anforderung zur Untersuchung einer Datei

Content-Type

application/octet-stream

Textkörper der Anforderung

Datei.

Beispielantwort:


```
{

  "completed": "Mon, 01 Mar 2021 06:54:39 GMT",

  "created": "Mon, 01 Mar 2021 06:54:38 GMT",

  "progress": 100,

  "scan_result": {

"noname": {
"started": "2021-03-01 06:54:39",
"stopped": "2021-03-01 06:54:39",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/b8eb4128-8cb4-4964-87cf-b9853e6544ec"
}
],
"verdict": "infected"
}

  },

  "status": "completed",

  "verdicts": [

"infected"

  ]

}
```


Anforderung zur Untersuchung mehrerer Dateien

Content-Type

multipart/form-data

Textkörper der Anforderung

Mehrere Dateien.

Beispielantwort:


```
{

  "completed": "Mon, 01 Mar 2021 06:55:44 GMT",

  "created": "Mon, 01 Mar 2021 06:55:43 GMT",

  "progress": 100,

  "scan_result": {

"clean": {
"started": "2021-03-01 06:55:43",
"stopped": "2021-03-01 06:55:43",
"verdict": "clean"
},
"corrupted.com": {
"errors": [
{
"error": "Corrupted object",
"object": "/root/kesl-service/tmp/75d28fe6-8154-4361-9382-90a76861518a"
}
],
"started": "2021-03-01 06:55:43",
"stopped": "2021-03-01 06:55:43",
"verdict": "non scanned"
},
"error.com": {
"errors": [
{
"error": "read error",
"object": "/root/kesl-service/tmp/37f6e0dd-13f9-4d11-899c-5fe0f23e407d"
}
],
"started": "2021-03-01 06:55:44",
"stopped": "2021-03-01 06:55:44",
"verdict": "non scanned"
```

```
},
"infected.com": {
"started": "2021-03-01 06:55:44",
"stopped": "2021-03-01 06:55:44",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/7d664646-bf56-4060-b958-5ce9e746c929"
}
],
"verdict": "infected"
}
  },

  "status": "completed",

  "verdicts": [

"clean",
"non scanned",
"infected"
  ]

}
```

Anforderung der Untersuchung von Docker-Images

Content-Type

text/plain

Textkörper der Anforderung

Link zum Docker-Image oder zu den Docker-Images, die untersucht werden sollen.

Folgende Werte sind möglich:

- Repository-Pfad zu einem Image (z. B. https://index.docker.io/jerbi/eicar:latest).
- Pfadmaske, die mehrere Images umfasst (z. B. https://index.docker.io/<name mask>:<tag mask>). Um eine Maske festzulegen, können Sie die folgenden Symbole verwenden: "?" und "*".

Beispielantwort:

```
{
  "completed": "Sun, 31 Jan 2021 10:29:26 GMT",
  "created": "Sun, 31 Jan 2021 10:29:20 GMT",
  "progress": 100,
  "scan_result": {
"jerbi/eicar:latest": {
"started": "2021-01-31 10:29:25",
"stopped": "2021-01-31 10:29:26",
"threats": [
{
"name": "EICAR-Test-File",
"object": "[image:docker.io/jerbi/eicar:latest] /eicar.com.txt"
}
],
"verdict": "infected"
}
  },
  "status": "completed",
  "verdicts": [
"infected"
  ]
}
```


Mögliche Fehler

Um eine Liste der Images anhand einer Maske abzurufen, wird eine Anforderung über die Docker-REST-API verwendet.

Allerdings ist diese Funktion auf vielen öffentlichen Servern aus Sicherheitsgründen deaktiviert. Der Versuch, auf solchen Servern Images nach Maske zu untersuchen, führt zu einem Fehler.

Beispiel für einen Fehler:


```
{
  "completed": "Mon, 01 Mar 2021 07:02:24 GMT",
```

```
  "created": "Mon, 01 Mar 2021 07:02:22 GMT",

  "scan_errors": [

{
"code": 401,
"details": {
"context": {
"image_mask": "/jerbi/eic*:latest",
"repository": "index.docker.io",
"repository_base": "index.docker.io"
},
"errors": [
"Unauthorized"
]
},
"message": "Invalid source"
},
[
"Unauthorized"
]
  ],

  "status": "completed"

}
```


Anforderung der Untersuchung von Docker-Images mit zusätzlichen Einstellungen

Content-Type

application/json

Textkörper der Anforderung

JSON der folgenden Art:


```
{

  "source": "https://index.docker.io/jerbi/eicar:latest",
```

```
  "params": {

"destination": "https://fake",
"skipimageifexists": true,
"custom_callbacks": {
"on_detect": {
"uri": "http://10.16.42.75:5050",
"content-type": "application/json",
"body": {
"session_id": "100",
"session_init": "20201105T072403+0300",
"infected_items": "$infected"
}
},
"on_complete": {
"body": {
"session_id": "100",
},
"uri": "http://10.16.42.75:5050/on_complete",
}
}
  }

}
```

Zusätzliche Einstellungen der Anforderung

Der Abschnitt `params` kann folgende Einstellungen enthalten:

- `destination` (optional) – Server, auf den das untersuchte Image kopiert werden soll.
- `skipimageifexists` (optional) – Image nicht untersuchen und nicht kopieren, wenn auf dem Zielserver bereits ein Image mit demselben Namen und der SHA256-Hash-Summe vorhanden ist; diese Einstellung kann nur angegeben werden, wenn die Einstellung `destination` vorhanden ist.
- `custom_callbacks` (optionaler Parameter) – Beschreibung von Anforderungen, die nach Abschluss der Untersuchung gesendet werden sollen:
  - on_detect – Die Anforderung wird gesendet, wenn eine Bedrohung gefunden wird.
  - on_complete – Die Anforderung wird immer nach Abschluss der Untersuchung gesendet.

In der Beschreibung des Textkörpers der Anforderung können Sie den Platzhalter `$infected` angeben, der mit der Liste der infizierten Objekte ersetzt wird.

Beispielantwort:

```
{
  "completed": "Mon, 01 Mar 2021 07:13:49 GMT",
  "created": "Mon, 01 Mar 2021 07:13:42 GMT",
  "progress": 100,
  "scan_errors": [
{
"code": 500,
"message": "Unable to get images hash from destination registry"
}
  ],
  "scan_params": {
"destination": "https://fake",
"skipimageifexists": true
  },
  "scan_result": {
"jerbi/eicar:latest": {
"started": "2021-03-01 07:13:48",
"stopped": "2021-03-01 07:13:49",
"threats": [
{
"name": "EICAR-Test-File",
"object": "[image:docker.io/jerbi/eicar:latest] /eicar.com.txt"
}
],
"verdict": "infected"
}
  },
  "status": "completed",
  "verdicts": [
"infected"
```

```
  ]

}
```

Anforderung zum Abruf von Informationen zu Untersuchungssitzungen (GET)

Ziel

Abruf von Informationen zu Untersuchungssitzungen

Pfad

http://<server>:<port>/scans[?force] – Anforderung zum Abruf einer Liste mit Sitzungen

http://<server>:<port>/scans/<eindeutige ID der Untersuchungssitzung>[?force] – Anforderung zum Abruf von Informationen zu einer bestimmten Sitzung

Einstellungen

Der KESL-Container speichert die Daten zu Untersuchungssitzungen in einer Datenbank mit Untersuchungsergebnissen.

Die optionale Einstellung `?force` initiiert das Lesen von Informationen aus der Datenbank im Fall, dass mehrere Instanzen des KESL-Containers dieselbe Datenbank verwenden. Fehlt die Einstellung, so werden nur Informationen zu Sitzungen angezeigt, die von einer bestimmten Instanz des KESL-Containers initiiert wurden.

Anforderung einer Liste der Untersuchungssitzungen

Pfad

http://<server>:<port>/scans[?force]

Beispielantwort:

```
{

  "629ae0a9-28de-4e2f-b130-67e87ba4d61d": {

"progress": 100,
"status": "completed"

  },
```

```
  "655b96fc-34ca-4915-9c41-d52724a277de": {

"progress": 100,
"status": "completed"

  },

  "7d27e9b4-a4d7-469b-bdcf-ebfe953498e4": {

"progress": 100,
"status": "completed"

  },

  "c32ca88f-2d24-47ec-b040-0540366bea4b": {

"progress": 100,
"status": "completed"

  },

  "df11ad81-26aa-42f9-94bb-39dee4304807": {

"progress": 0,
"status": "completed"

  },

  "fa25340f-4898-497f-ab59-8df494f4ea47": {

"progress": 100,
"status": "completed"

  }

}
```

Anforderung zum Abruf von Informationen zu einer bestimmten Sitzung

Pfad

http://<server>:<port>/scans/<eindeutige ID der Untersuchungssitzung>[?force]

Beispielantwort:

```
{
```

```
  "completed": "Mon, 01 Mar 2021 06:45:19 GMT",

  "created": "Mon, 01 Mar 2021 06:45:19 GMT",

  "progress": 100,

  "scan_result": {

"noname": {
"started": "2021-03-01 06:45:19",
"stopped": "2021-03-01 06:45:19",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/65b55d89-b758-4609-a2f3-f63ef839815d"
}
],
"verdict": "infected"
}

  },

  "status": "completed",

  "verdicts": [

"infected"

  ]

}
```


Anforderung zum Hinzufügen eines Registrierungszertifikats (POST)

Ziel

Hinzufügen eines Registrierungszertifikats ohne Neustart des KESL-Containers.

Pfad

http://<server>:<port>/addcert

Header der Anforderung

Die Anforderung enthält den Header "Content-Type".

Unterstützte Werte:

- application/octet-stream – eine einzige Zertifikatsdatei
- multipart/form-data – mehrere Zertifikatsdateien

Anfrage zum Abrufen von Informationen zum Status des KESL-Containers (GET)

Ziel

Abrufen von Informationen über den aktuellen Status des KESL-Containers und über die Statusparameter der App, von denen der Status des KESL-Containers abhängt (App-, Lizenz- und Datenbankenstatus).

Pfad

http://<Server>:<Port>/status

Beispielantwort:

```
{'product info': {'databases_date': '<Release-Datum der Datenbank>',
'databases_loaded': True, 'license_expiration': '<Ablaufdatum der Lizenz>',
'license_info': 'The key is valid', 'policy': 'Not applied', 'version': '<Version der
App>'}, 'status': 'service available'}
```

Mögliche Fehler

Ein Beispiel für einen Fehler (die App wurde im KESL-Container nicht gestartet):

```
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'service not available', 'status_reason': ['KESL not response']}
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'service not available', 'status_reason': ['KESL not response']}
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'service not available', 'status_reason': ['KESL not response']}
```

Beispiel für eine Fehlerausgabe (App-Datenbanken nicht heruntergeladen):

```
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': '<Ablaufdatum der Lizenz>', 'license_info': 'Inconsistent
update', 'policy': 'Not applied', 'version': '<Version der App>'}, 'status': 'service
not available', 'status_reason': ['Databases not loaded', 'License error: Inconsistent
update']}
```

Beispiel für eine Fehlerausgabe (Ablaufdatum der Lizenz abgelaufen):

{'product info': {'databases_date': '<Release-Datum der Datenbank>',
'databases_loaded': True, 'license_expiration': '< Ablaufdatum der Lizenz >',
'license_info': 'Expired', 'policy': 'Not applied', 'version': '<KESL-Version>'},
'status': 'service not available', 'status_reason': ['License error: Expired']}

Kontaktieren Sie den technischen Support

Sollten Sie in der Dokumentation und oder in anderen Informationsquellen für die App keine Lösung für Ihr Problem finden, empfehlen wir Ihnen, sich an den Technischen Support zu wenden. Die Mitarbeiter des Technischen Support beantworten Ihre Fragen zur Installation und Verwendung von Kaspersky Endpoint Security.

Kaspersky bietet Support während des gesamten Lebenszyklus von Kaspersky Endpoint Security (siehe die Seite zum Lebenszyklus von Apps). Bitte machen Sie sich mit den Support-Richtlinien vertraut, bevor Sie sich an den Technischen Support wenden.

Eine Kontaktaufnahme mit den Support-Experten ist auf folgende Weise möglich:

- Aufrufen der Webseite des Technischen Supports.
- Anfrage an den Technischen Support von Kaspersky über das Portal Kaspersky CompanyAccount

Technischer Support über das Kaspersky CompanyAccount

Kaspersky CompanyAccount – Ein Webdienst für Unternehmen, die Apps von Kaspersky verwenden. Das Portal Kaspersky CompanyAccount dient der Kontaktaufnahme mit den Spezialisten von Kaspersky über elektronische Anfragen. Im Portal Kaspersky CompanyAccount können Sie den Status der Bearbeitung von E-Mail-Anfragen durch die Kaspersky-Experten verfolgen und die Chronik der E-Mail-Anfragen speichern.

Sie können alle Mitarbeiter Ihrer Organisation im Rahmen eines Benutzerkontos für Kaspersky CompanyAccount registrieren. Mithilfe eines Benutzerkontos können Sie die elektronischen Anfragen der registrierten Mitarbeiter an Kaspersky zentral kontrollieren, sowie die Berechtigungen dieser Mitarbeiter für Kaspersky CompanyAccount verwalten.

Das Portal Kaspersky CompanyAccount ist in folgenden Sprachen verfügbar:

- Englisch
- Spanisch
- Italienisch
- Deutsch
- Polnisch
- Portugiesisch
- Russisch
- Französisch
- Japanisch

Weitere Informationen zu Kaspersky CompanyAccount erhalten Sie auf der Website des Technischen Supports.

Informationen für den Technischen Support abrufen

Nachdem Sie die Spezialisten des Technischen Supports von Kaspersky über ein Problem informiert haben, werden Sie möglicherweise aufgefordert, *eine Ablaufverfolgungs-Datei* oder *eine Dump-Datei* zu senden.

Darüber hinaus können die Spezialisten des Technischen Supports zusätzliche Informationen zum Betriebssystem und zu laufenden Prozessen auf dem Gerät, sowie detaillierte Berichte zur Ausführung der App-Komponenten anfordern.

Während der Diagnose werden Sie möglicherweise von Spezialisten des Technischen Supports dazu aufgefordert, die folgenden Einstellungen der App zu ändern:

- Die Funktionalität zum Abrufen erweiterter Diagnoseinformationen aktivieren.
- Die Ausführung einzelner App-Komponenten, die nicht über Standard-Tools der Benutzeroberfläche verfügbar sind, feiner abstimmen.
- Die Speichereinstellungen der empfangenen Diagnoseinformationen ändern.
- Das Abfangen des Netzwerkverkehrs und dessen Speichern in einer Datei konfigurieren.

Alle Informationen, die zum Ausführen der oben genannten Maßnahmen erforderlich sind (eine Beschreibung der Schrittfolge, veränderbare Parameter, Konfigurationsdateien, Skripte, zusätzliche Befehlszeilenoptionen, Debug-Module, spezielle Tools usw.) sowie eine Zusammenstellung der erhaltenen Daten des Debug-Modus, werden Ihnen von den Spezialisten des Technischen Supports mitgeteilt. Die erhaltenen erweiterten Diagnoseinformationen werden auf dem Gerät des Benutzers gespeichert. Die erhaltenen Daten werden nicht automatisch an Kaspersky weitergeleitet.

Die oben aufgeführten Maßnahmen dürfen nur unter Anleitung der Spezialisten des Technischen Supports und gemäß der von ihnen erhaltenen Anweisungen durchgeführt werden. Wenn die Ausführungseinstellungen auf eine andere Weise geändert werden, als in der Dokumentation zur App oder in den Anleitungen der Support-Experten beschrieben, so kann die App oder das Betriebssystem verlangsamt oder beeinträchtigt werden, das Schutzniveau sinken und der Zugriff auf und die Integrität von Informationen beschädigt werden.

Über Protokolldateien der App

Mit einer *Protokolldatei* von Kaspersky Endpoint Security können Sie die schrittweise Ausführung von App-Befehlen verfolgen und erkennen, in welcher Phase der App-Ausführung ein Fehler auftritt.

Standardmäßig werden keine Protokolldateien der App erstellt. Sie können die Erstellung von Protokolldateien der App aktivieren oder deaktivieren und den Detaillierungsgrad der Protokolldateien in der Befehlszeile mithilfe der allgemeinen App-Einstellungen sowie der grafischen Benutzeroberfläche konfigurieren.

Wenn Sie die Erstellung von Protokolldateien der App aktiviert haben, werden die Protokolldateien standardmäßig im Verzeichnis /var/log/kaspersky/kesl/ gespeichert. Für den Zugriff auf dieses Verzeichnis sind Root-Rechte erforderlich.

Protokolldateien werden auf dem Gerät gespeichert, solange die App verwendet wird. Bei der Deinstallation der App werden sie dauerhaft gelöscht. Es werden keine Protokolldateien automatisch an Kaspersky gesendet.

Protokolldateien werden in lesbarer Form gespeichert. Es wird empfohlen, die Informationen bis zu ihrer Übermittlung an Kaspersky vor unbefugtem Zugriff zu schützen.

Inhalt von Protokolldateien der App

Die Protokolldateien enthalten die folgenden allgemeinen Informationen:

- Ereigniszeit
- Nummer des ausführenden Threads
- App-Komponente, die das Ereignis verursacht hat
- Signifikanz des Ereignisses (informatives Ereignis, Warnung, kritisches Ereignis, Fehler)
- Eine Beschreibung des Ereignisses, bei dem ein Befehl von einer App-Komponente ausgeführt wird, und das Ergebnis der Ausführung dieses Befehls

Protokolldateien können zusätzlich zu den allgemeinen Daten die folgenden Informationen enthalten:

- Status der App-Komponenten und Daten zu ihrer Ausführung
- Daten zur Benutzeraktivität in der App
- Daten zur Hardware, die auf dem Gerät installiert ist
- Daten zu beliebigen Objekten und Ereignissen des Betriebssystems, sowie Informationen zur Benutzeraktivität
- Daten, die in den Objekten des Betriebssystems enthalten sind (z. B. der Inhalt von Dateien, die möglicherweise persönliche Daten des Benutzers enthalten)
- Daten des Netzwerkverkehrs (z. B. der Inhalt der Eingabefelder auf einer Website, die Bankkartendaten oder andere sensible Daten enthalten können)
- Von Kaspersky-Servern empfangene Daten (z. B. die Version der App-Datenbanken)
- Daten, die von KATA-Servern empfangen werden.
- Daten über benötigte CPU-Ressourcen
- Daten über benötigte RAM-Ressourcen
- Daten über von Anwendungen durchgeführte Lesen- und Schreibvorgängen mit
- Daten über die Menge der zwischengespeicherten Informationen, die für die Ausführung der App erforderlich sind.

Protokolleinstellungen der App konfigurieren

Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center verwalten, können Sie die Einstellungen für die Ablaufverfolgung in den Einstellungen der Richtlinie von Kaspersky Endpoint Security entweder über die Web Console oder die Verwaltungskonsole konfigurieren.

Wenn Sie die App über die Befehlszeile verwalten, können Sie die Einstellungen für die Ablaufverfolgung der App in den allgemeinen App-Einstellungen konfigurieren.

Konfiguration der Ablaufverfolgung in der Web Console

In der Web Console können Sie Einstellungen für die Ablaufverfolgung der App in den Richtlinieneinstellungen konfigurieren (**App-Einstellungen** → **Allgemeine Einstellungen** → **App-Einstellungen** → Abschnitt **Protokollierungs- und Dump-Einstellungen**) (siehe untere Tabelle).

Parameter für die Ablaufverfolgung der App

Einstellung	Beschreibung
Pfad zum Verzeichnis der Protokolldatei	Eingabefeld für den Pfad zum Verzeichnis, in dem die Protokoll-Dateien gespeichert werden. Standardwert: /var/log/kaspersky/kesl. Wenn Sie ein anderes Verzeichnis angeben, stellen Sie sicher, dass das Benutzerkonto, unter dem Kaspersky Endpoint Security ausgeführt wird, eine Lese- und Schreibberechtigung für dieses Verzeichnis besitzt. Für den Zugriff auf das Standardverzeichnis zum Speichern von Ablaufverfolgungsdateien sind Root-Rechte erforderlich.
Maximale Anzahl an Protokolldateien	Eingabefeld für die maximale Anzahl an Protokolldateien der App. Standardwert: 10.
Maximale Größe der Protokolldatei (MB)	Eingabefeld für die maximale Größe der Protokolldateien der App (in Megabyte). Standardwert: 500.

Sie müssen die App neu starten, um die Einstellungen für die Ablaufverfolgung der App anzuwenden.

Konfiguration der Ablaufverfolgung in der Verwaltungskonsole

In der Verwaltungskonsole können Sie Einstellungen für die Ablaufverfolgung der App in den Richtlinieneinstellungen konfigurieren (**Allgemeine Einstellungen** → **App-Einstellungen**).

Wenn Sie im Block **Protokollierungs- und Dump-Einstellungen** auf den Link **Konfigurieren** klicken, öffnet sich ein Fenster, in dem Sie Einstellungen der Ablaufverfolgung konfigurieren können (siehe untere Tabelle).

Parameter für die Ablaufverfolgung der App

Einstellung	Beschreibung
Pfad zum Verzeichnis der Protokolldatei	Eingabefeld für den Pfad zum Verzeichnis, in dem die Protokoll-Dateien gespeichert werden. Standardwert: /var/log/kaspersky/kesl.

	Wenn Sie ein anderes Verzeichnis angeben, stellen Sie sicher, dass das Benutzerkonto, unter dem Kaspersky Endpoint Security ausgeführt wird, eine Lese- und Schreibberechtigung für dieses Verzeichnis besitzt. Für den Zugriff auf das Standardverzeichnis zum Speichern von Ablaufverfolgungsdateien sind Root-Rechte erforderlich.
Maximale Größe der Protokolldatei (MB)	Eingabefeld für die maximale Größe der Protokolldateien der App (in Megabyte). Standardwert: 500.
Maximale Anzahl an Protokolldateien	Eingabefeld für die maximale Anzahl an Protokolldateien der App. Standardwert: 10.

Sie müssen die App neu starten, um die Einstellungen für die Ablaufverfolgung der App anzuwenden.

Konfiguration der Ablaufverfolgung über die Befehlszeile

Über die Befehlszeile können Sie die Einstellungen für Ablaufverfolgung der App in den allgemeinen Anwendungseinstellungen mithilfe der Parameter `TraceLevel`, `TraceFolder`, `TraceMaxFileCount` und `TraceMaxFileSize` konfigurieren.

Mit dem Parameter `TraceLevel` können Sie die Erstellung von Ablaufverfolgungen für die App aktivieren oder deaktivieren und die Detailstufe innerhalb der Ablaufverfolgungsdateien angeben. Der Parameter kann die folgenden Werte annehmen:

- `Detailed` – detaillierteste Protokolldateien erstellen
- `MediumDetailed` – Protokolldatei mit Info- und Fehlermeldungen erstellen
- `NotDetailed` – Protokolldatei mit Fehlermeldungen erstellen
- `None` (Standardwert) – keine Protokolldatei erstellen

Mit dem Parameter `TraceFolder` können Sie das Verzeichnis angeben, in dem die Ablaufverfolgungsdateien der App gespeichert werden. Standardwert: /var/log/kaspersky/kesl. Wenn Sie ein anderes Verzeichnis angeben, stellen Sie sicher, dass das Benutzerkonto, unter dem Kaspersky Endpoint Security ausgeführt wird, eine Lese- und Schreibberechtigung für dieses Verzeichnis besitzt. Für den Zugriff auf das Standardverzeichnis zum Speichern von Ablaufverfolgungsdateien sind Root-Rechte erforderlich.

Mit dem Parameter `TraceMaxFileCount` können Sie die Maximalanzahl an Ablaufverfolgungsdateien der App angeben Der Parameter kann Werte von 1 bis 10.000 annehmen. Standardwert: 10.

Mit dem Parameter `TraceMaxFileSize` können Sie die maximale Größe der Ablaufverfolgungsdateien der App angeben (in Megabtye). Der Parameter kann Werte von 1 bis 1000 annehmen. Standardwert: 500.

Sie können den Wert von Parametern mithilfe von Befehlszeilenschaltern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen App-Einstellungen enthält.

Nach dem Ändern der Werte für die Parameter `TraceFolder`, `TraceMaxFileCount` und `TraceMaxFileSize` müssen Sie die App neu starten.

Über Protokolldateien der Verwaltungs-Plug-ins für die App

Es werden keine Protokolldateien der Verwaltungs-Plug-ins automatisch an Kaspersky gesendet.

Protokolldateien werden in lesbarer Form gespeichert. Es wird empfohlen, die Informationen bis zu ihrer Übermittlung an Kaspersky vor unbefugtem Zugriff zu schützen.

Protokolldateien des MMC-Verwaltungs-Plug-ins

Wenn Sie zur Verwaltung von Kaspersky Endpoint Security die Verwaltungskonsole verwenden, können Informationen über Ereignisse während der Ausführung des MMC-Verwaltungs-Plug-ins in der Protokolldatei des MMC-Plug-ins für Kaspersky Endpoint Security auf dem Gerät aufgezeichnet werden, auf dem der Administrationsserver installiert ist. Der Dateiname enthält die Versionsnummer der App, das Datum und die Uhrzeit der Erstellung der Datei sowie die Prozess-ID (PID). Diese Datei zeichnet Informationen über Ereignisse auf, die während der Ausführung des mmc-basierte Plug-ins auftreten, insbesondere über die Ausführung von Richtlinien und Aufgaben.

Standardmäßig werden für das MMC-Plug-in keine Protokolldateien erstellt. Mithilfe von Registrierungsschlüsseln können Sie eine Protokolldatei für das mmc-basierte Plug-in anlegen. Für weitere ausführliche Informationen zum Anlegen von Protokolldateien können Sie sich an den Technischen Support wenden.

Alle erstellten Protokolldateien des mmc-basierten Plug-ins befinden sich in dem Ordner, den der Benutzer beim Festlegen der Registrierungsschlüssel angegeben hat.

Protokolldateien des Web-Plug-ins

Wenn Sie Web Console zur Verwaltung von Kaspersky Endpoint Security verwenden, können Informationen über Ereignisse während der Ausführung des Web-Verwaltungs-Plug-ins in den Protokolldateien des Web-Plug-ins aufgezeichnet werden.

Protokolldateien des Web-Plug-ins werden automatisch erstellt, wenn im Installationsassistenten von Web Console die Protokollierung im Aktivitätsprotokoll von Web Console aktiviert ist (weitere Informationen dazu finden Sie in der Hilfe von Kaspersky Security Center).

Die Protokolldateien des Web-Plug-ins werden im Installationsordner der Web Console im Unterordner "logs" gespeichert.

Inhalt der Protokolldateien der Verwaltungs-Plug-ins

Die Protokolldateien enthalten die folgenden allgemeinen Informationen:

- Ereigniszeit
- Nummer des ausführenden Threads
- App-Komponente, die das Ereignis verursacht hat
- Signifikanz des Ereignisses (informatives Ereignis, Warnung, kritisches Ereignis, Fehler)

- Eine Beschreibung des Ereignisses, bei dem ein Befehl von einer App-Komponente ausgeführt wird, und das Ergebnis der Ausführung dieses Befehls

Neben allgemeinen Daten können Protokolldateien die folgenden Informationen enthalten:

- Personenbezogene Daten, einschließlich Nachname, Vorname und Vatersname, wenn diese Daten Teil des Pfads zu den Dateien sind
- Der Kontoname zur Anmeldung am Betriebssystem, wenn der Kontoname Teil des Dateinamens ist.

Über Dump-Dateien

Eine *Dump-Datei* enthält alle Informationen zum Arbeitsspeicher der Prozesse von Kaspersky Endpoint Security zum Zeitpunkt der Erstellung der Dump-Datei. Standardmäßig werden keine Dump-Dateien erstellt. Sie können die Erstellung einer Dump-Datei im Falle eines App-Absturzes aktivieren oder deaktivieren.

Wenn Sie die Dump-Erstellung aktiviert haben, werden die Dump-Dateien standardmäßig in den Verzeichnissen /var/opt/kaspersky/kesl/common/dumps und /var/opt/kaspersky/kesl/common/dumps-user gespeichert.

Für den Zugriff auf Dump-Dateien sind Root-Rechte erforderlich.

Dump-Dateien werden auf dem Gerät gespeichert, solange die App verwendet wird. Bei der Deinstallation der App werden sie dauerhaft gelöscht. Es werden keine Dump-Dateien automatisch an Kaspersky gesendet.

Dump-Dateien können persönliche Daten enthalten. Es wird empfohlen, die Informationen bis zu ihrer Übermittlung an Kaspersky vor unbefugtem Zugriff zu schützen.

Dump-Erstellung aktivieren und deaktivieren

Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center verwalten, können Sie die Dump-Erstellung in den Einstellungen der Richtlinie von Kaspersky Endpoint Security entweder in der Web Console oder in der Verwaltungskonsole aktivieren oder deaktivieren.

Wenn Sie die App über die Befehlszeile verwalten, können Sie die Dump-Erstellung mithilfe der Konfigurationsdatei kesl.ini aktivieren oder deaktivieren.

Die maximale Anzahl von Dump-Dateien ist begrenzt.

In Abhängigkeit von den Betriebssystem-Einstellungen werden möglicherweise keine benutzerdefinierten Dump-Dateien erstellt. Stellen Sie sicher, dass das folgende Parameter-Wert-Paar angegeben ist: `sysctl kernel.yama.ptrace_scope=0`.

Dump-Erstellung in der Web Console aktivieren und deaktivieren

In der Web Console können Sie die Dump-Erstellung in den Richtlinieneigenschaften aktivieren oder deaktivieren (**App-Einstellungen** → **Allgemeine Einstellungen** → **App-Einstellungen** → Abschnitt **Protokollierungs- und Dump-Einstellungen**).

Einstellungen der Dump-Erstellung

Einstellung	Beschreibung
Im Falle eines App-Absturzes einen Dump erstellen	Das Kontrollkästchen aktiviert oder deaktiviert die Erstellung einer Dump-Datei, wenn die App abstürzt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Pfad zum Verzeichnis mit der Dump-Datei.	Eingabefeld für den Pfad zum Verzeichnis, in dem die Dump-Dateien gespeichert werden. Die Eingabefeld nimmt maximal 128 Zeichen auf. Standardwert: /var/opt/kaspersky/kesl/common/dumps.

Sie müssen die App neu starten, um die Einstellungen zum Erstellen eines Dumps anzuwenden.

Dump-Erstellung in der Verwaltungskonsole aktivieren und deaktivieren

In der Verwaltungskonsole können Sie die Erstellung von Dump-Dateien in den Richtlinieneigenschaften aktivieren und deaktivieren (**Allgemeine Einstellungen** → **App-Einstellungen**).

Wenn Sie im Block **Protokollierungs- und Dump-Einstellungen** auf den Link **Konfigurieren** klicken, öffnet sich ein Fenster, in dem Sie Dump-Erstellung konfigurieren können.

Einstellungen der Dump-Erstellung

Einstellung	Beschreibung
Im Falle eines App-Absturzes einen Dump erstellen	Das Kontrollkästchen aktiviert oder deaktiviert die Erstellung einer Dump-Datei, wenn die App abstürzt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Pfad zum Verzeichnis mit der Dump-Datei.	Eingabefeld für den Pfad zum Verzeichnis, in dem die Dump-Dateien gespeichert werden. Die Eingabefeld nimmt maximal 128 Zeichen auf. Standardwert: /var/opt/kaspersky/kesl/common/dumps.

Sie müssen die App neu starten, um die Einstellungen zum Erstellen eines Dumps anzuwenden.

Dump-Erstellung über die Befehlszeile aktivieren und deaktivieren

So aktivieren oder deaktivieren Sie die Dump-Erstellung mithilfe der Konfigurationsdatei kesl.ini:

1. Beenden Sie Kaspersky Endpoint Security.
2. Öffnen Sie die Datei /var/opt/kaspersky/kesl/common/kesl.ini zur Bearbeitung.
3. Legen Sie im Abschnitt **[General]** den Parameterwert fest:
   - `CoreDumps=yes` – Dump-Erstellung im Falle eines App-Absturzes aktivieren.
   - `CoreDumps=no` – Dump-Erstellung deaktivieren.
4. Wenn Sie das Standardverzeichnis ändern möchten, in dem Dump-Dateien gespeichert werden, geben Sie den Verzeichnispfad im Parameter `CoreDumpsPath` an.

5. Starten Sie Kaspersky Endpoint Security.

Über die Ferndiagnose von Geräten mithilfe von Kaspersky Security Center

In Kaspersky Security Center können Sie eine Ferndiagnose von Client-Geräten durchführen. Mit dem Ferndiagnoseverfahren können Sie die folgenden Operationen aus der Ferne durchführen:

- Protokollierung aktivieren und deaktivieren
- Protokollierungsgrad ändern
- Protokolldateien herunterladen
- Protokoll der Remote-Installationen der App herunterladen
- Ereignisprotokolle des Systems (syslog) herunterladen
- Apps starten, beenden und neu starten

Ferndiagnose über Web Console

Wenn Sie Kaspersky Endpoint Security über Web Console verwalten, wird die Ferndiagnose des Client-Geräts im Fenster zur Ferndiagnose durchgeführt.

So öffnen Sie das Fenster zur Ferndiagnose des Geräts:

1. Wählen Sie im Hauptfenster von Web Console **Assets (Geräte)** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie das Gerät aus, für das Sie eine Ferndiagnose durchführen möchten, und klicken Sie auf den Gerätenamen.

   Das Eigenschaftenfenster des Geräts wird geöffnet.

3. Wählen Sie auf der Registerkarte **Erweitert** den Abschnitt **Ferndiagnose**.

Im Fenster zur Ferndiagnose des Geräts können Sie das Remote-Installationsprotokoll der App anzeigen.

So zeigen Sie das Remote-Installationsprotokoll der App auf einem Gerät an:

1. Öffnen Sie das Fenster zur Ferndiagnose des Geräts:

2. Klicken Sie auf der Registerkarte **Ereignisprotokolle** im Block **Protokolldateien** auf den Link **Remote-Installationsprotokolle**.

   Das Fenster **Ereignisprotokolle des Geräts** wird geöffnet.

Weitere Informationen über Ferndiagnosen finden Sie in der Hilfe zu Kaspersky Security Center.

Ferndiagnose über die Verwaltungskonsole

Wenn Sie Kaspersky Endpoint Security über die Verwaltungskonsole verwalten, wird die Ferndiagnose mit dem speziellen Ferndiagnose-Tool von Kaspersky Security Center durchgeführt, das automatisch zusammen mit der Verwaltungskonsole auf dem Gerät installiert wird.

So öffnen Sie das Hauptfenster des Ferndiagnose-Tools für das Gerät:

1. Wählen Sie in der Struktur der Verwaltungskonsole im Ordner **Verwaltete Geräte** die Administrationsgruppe aus, die das benötigte Gerät enthält.
2. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.
3. Wählen Sie in der Liste der verwalteten Geräte das Gerät aus, mit dem Sie das Ferndiagnose-Tool verbinden möchten, und wählen Sie im Kontextmenü des Geräts **Externe Tools → Ferndiagnose** aus.

   Das Hauptfenster des Ferndiagnose-Tools **Kaspersky Security Center Ferndiagnose-Tool** wird geöffnet.

Mithilfe des Tools zur Ferndiagnose des Geräts können Sie das Remote-Installationsprotokoll der App anzeigen.

So zeigen Sie das Remote-Installationsprotokoll der App auf einem Gerät an:

1. Öffnen Sie das Hauptfenster für die Ferndiagnose des Geräts.
2. Konfigurieren Sie bei Bedarf die Einstellungen für die Verbindung des Tools mit dem Gerät. Klicken Sie im Hauptfenster des Ferndiagnose-Tools auf die Schaltfläche **Anmelden**.
3. Wählen Sie im Objektbaum des neuen Fensters den Ordner **Remote-Installationsprotokolle** aus.

Weitere Informationen über das Ferndiagnose-Tool finden Sie in der Hilfe zu Kaspersky Security Center.

Verbindung zum Administrationsserver manuell überprüfen. Tool klnagchk

Im Lieferumfang des Administrationsagenten ist das Tool klnagchk enthalten, mit dem die Verbindung zum Administrationsserver geprüft werden kann.

Nach der Installation des Administrationsagenten befindet sich das Tool in 32-Bit-Betriebssystemen im Verzeichnis/opt/kaspersky/klnagent/bin und in 64-Bit-Betriebssystemen im Verzeichnis /opt/kaspersky/klnagent64/bin. Abhängig von den verwendeten Schlüsseln werden vom Administrationsagenten beim Start folgenden Aktionen ausgeführt:

- In die Ereignisprotokolldatei schreiben oder die Werte der Einstellungen für die Verbindung des auf dem Client-Gerät installierten Administrationsagenten mit dem Administrationsserver anzeigen.
- In die Ereignisprotokolldatei schreiben oder die Statistiken des Administrationsagenten (seit seinem letzten Start) und die Ergebnisse der Ausführung des Tools anzeigen.
- Es wird versucht, eine Verbindung zwischen dem Administrationsagenten und dem Administrationsserver herzustellen.
- Wenn keine Verbindung hergestellt werden kann, sendet das Tool ein ICMP-Paket, um den Status des Geräts, auf dem der Administrationsserver installiert ist, zu prüfen.

Die Syntax des Tools lautet

```
klnagchk [-logfile <Dateiname>] [-sp] [-savecert <Pfad zur Zertifikatsdatei>] [-restart]
```

Beschreibung der Schlüssel

- `-logfile <Dateiname>` – Einstellungswerte der Verbindung zwischen dem Administrationsagenten und dem Server sowie die Ergebnisse der Ausführung des Tools in einer Datei des Ereignisprotokolls speichern. Wenn dieser Schlüssel nicht verwendet wird, werden Einstellungen, Ergebnisse und Fehlermeldungen auf dem Bildschirm ausgegeben.

- `-sp` – Kennwort für die Authentifizierung des Benutzers auf dem Proxy-Server anzeigen. Diese Einstellung wird verwendet, wenn die Verbindung zum Administrationsserver über einen Proxy-Server hergestellt wird.

- `-savecert <Dateiname>` – Zertifikat für die Authentifizierung des Zugriffs zum Administrationsserver in der angegebenen Datei speichern.

- `-restart` – Administrationsagent neu starten.

Verbindung zum Administrationsserver manuell herstellen. Tool klmover

Im Lieferumfang des Administrationsagenten ist das Tool klmover enthalten, mit dem die Verbindung zum Administrationsserver verwaltet werden kann.

Nach der Installation des Administrationsagenten befindet sich das Tool in 32-Bit-Betriebssystemen im Verzeichnis/opt/kaspersky/klnagent/bin und in 64-Bit-Betriebssystemen im Verzeichnis /opt/kaspersky/klnagent64/bin. Abhängig von den verwendeten Schlüsseln werden vom Administrationsagenten beim Start folgenden Aktionen ausgeführt:

- Stellt eine Verbindung zwischen dem Administrationsagenten und dem Administrationsserver mit den angegebenen Einstellungen her

- In eine Ereignisprotokolldatei schreiben oder die Ergebnisse einer Operation anzeigen

Die Syntax des Tools lautet

```
klmover [-logfile <Dateiname>] {-address <Serveradresse>} [-pn <Portnummer>] [-ps <SSL-Portnummer>] [-nossl] [-cert <Pfad zur Zertifikatsdatei>] [-silent] [-dupfix]
```

Beschreibung der Schlüssel

- `-logfile <Dateiname>` – Ergebnisse der Ausführung des Tools in der angegebenen Datei speichern. Wenn dieser Schlüssel nicht verwendet wird, werden die Ergebnisse und Fehlermeldungen auf stdout ausgegeben.

- `-address <Serveradresse>` – Adresse des Administrationsservers der Verbindung. Als Adresse können IP-Adresse, NetBIOS oder DNS-Name des Geräts angegeben werden.

- `-pn <Portnummer>` – Nummer des Ports, über den eine ungesicherte Verbindung zum Administrationsserver hergestellt wird. Standardmäßig wird Port 14000 verwendet.

- `-ps <SSL-Portnummer>` – Nummer des SSL-Ports, über den eine sichere Verbindung zum Administrationsserver unter Verwendung des SSL-Protokolls hergestellt wird. Standardmäßig wird Port 13000 verwendet.

- `-nossl` – Ungesicherte Verbindung zum Administrationsserver verwenden. Wenn dieser Schlüssel nicht angegeben ist, wird die Verbindung des Agenten zum Server über das SSL-Protokoll hergestellt.

- `-cert <Pfad zur Zertifikatsdatei>` – Angegebene Zertifikatsdatei für die Authentifizierung des Zugriffs auf den neuen Administrationsserver verwenden. Wenn dieser Schlüssel nicht verwendet wird, erhält der Administrationsagent das Zertifikat bei der ersten Verbindung zum Administrationsserver.

- `-silent` – Tool im nicht interaktiven Modus starten. Es kann sinnvoll sein, diesen Schlüssel zu verwenden, wenn das Tool beispielsweise im entsprechenden Szenario bei der Registrierung des Benutzers gestartet wird.

- `-dupfix` – Dieser Schlüssel wird verwendet, wenn der Administrationsagent nicht wie gewohnt mithilfe eines Installationspakets installiert wurde, sondern beispielsweise aus einem Disk-Image wiederhergestellt wurde.

- `-cloningmode 1` – Wechselt in den Cloning-Modus.

- `-cloningmode 0` – Wechselt aus dem Cloning-Modus.

Anhänge

Dieser Abschnitt enthält Informationen, die den Haupttext der Hilfe ergänzen.

Anhang 1. Optimierung der Ressourcenauslastung

Bei der Untersuchung von Objekten verwendet Kaspersky Endpoint Security CPU-Ressourcen, die Eingabe/Ausgabe des Datenträger-Subsystems sowie den Arbeitsspeicher.

Um den Ressourcenverbrauch der App anzuzeigen, führen Sie folgenden Befehl aus:

```
top -bn1|grep kesl
```

Sie müssen den Befehl zum Zeitpunkt der Auslastung des Systems ausführen.

Die Ausgabe des Befehls zeigt den belegten Speicher und die verbrauchte Prozessorzeit an:

```
651 root 20 0 3014172 2.302g 154360 S 120.0 30.0 0:32.80 kesl
```

In Spalte 6 wird die Größe des residenten Speichers angezeigt: `2.302g`.

In Spalte 9 wird als Prozentsatz der Prozessorkernauslastung der Wert 120.0 angezeigt, wobei jeder einzelne Kern 100 Prozent entspricht. Ein Wert von 120 % bedeutet also, dass ein Kern voll und der andere zu 20 % ausgelastet ist.

Wenn der Betrieb von Kaspersky Endpoint Security während der Untersuchung von Objekten das System kritisch verlangsamt, muss die App konfiguriert werden, um die Nutzung der Systemressourcen zu optimieren.

Aufgabe identifizieren, welche Ressourcen verbraucht

Um zu bestimmen, welche Aufgabe oder Aufgaben der App die Systemressourcen beanspruchen, muss der Ressourcenverbrauch der Aufgabe zum Schutz vor bedrohlichen Dateien (vom Typ OAS) separat von den Aufgaben zur Untersuchung auf Befehl (vom Typ ODS und ContainerScan) betrachtet werden.

Wenn die App durch eine Richtlinie von Kaspersky Security Center verwaltet wird, muss für die Dauer dieser Überprüfung die Verwaltung lokaler Aufgaben zugelassen werden.

Analyse der Ausführung der Aufgabe zum Schutz vor bedrohlichen Dateien

So analysieren Sie die Ausführung der Aufgabe zum Schutz vor bedrohlichen Dateien:

1. Beenden Sie alle Untersuchungs- und Überwachungsaufgaben.
2. Stellen Sie sicher, dass die Aufgaben zur Untersuchung auf Befehl nicht während dieser Überprüfung und nicht nach Zeitplan gestartet werden. Sie können dies über Kaspersky Security Center oder lokal tun, indem Sie die folgenden Schritte ausführen:

a. Rufen Sie eine Liste mit allen Aufgaben der App ab, indem Sie den folgenden Befehl ausführen:

```
kesl-control --get-task-list
```

b. Führen Sie den folgenden Befehl aus, um die Zeitplaneinstellungen für die Aufgabe zur Schadsoftware-Untersuchung abzurufen:

```
kesl-control --get-schedule <Aufgaben-ID>
```

Wenn der Befehl `RuleType=Manual` ausgibt, wird die Aufgabe nur manuell ausgeführt.

c. Rufen Sie die Zeitplaneinstellungen für alle Aufgaben zur Schadsoftware-Untersuchung und zu benutzerdefinierten Untersuchung (falls vorhanden) ab und legen Sie mit dem folgenden Befehl deren manuellen Start fest:

```
kesl-control --set-schedule <Aufgaben-ID> RuleType=Manual
```

3. Aktivieren Sie die Erstellung von Ablaufverfolgungsdateien mit hohem Detaillierungsgrad für die App, indem Sie den folgenden Befehl ausführen:

```
kesl-control --set-app-settings TraceLevel=Detailed
```

4. Starten Sie mit dem folgenden Befehl die Aufgabe zum Schutz vor bedrohlichen Dateien, falls diese nicht bereits läuft:

```
kesl-control --start-task 1
```

5. Sorgen Sie für eine Systemauslastung im gleichen Modus, der die Leistungsprobleme verursacht hat. Es genügen einige Stunden.

Im Rahmen seiner Auslastung speichert die App viele Informationen in den Protokolldateien. Dabei werden standardmäßig 5 Dateien mit je 500 MB angelegt und die ältesten Informationen überschrieben. Sollten die Probleme mit der Leistung und dem Ressourcenverbrauch dieses Mal nicht auftreten, sind höchstwahrscheinlich die Aufgaben zur Untersuchung auf Befehl für solche Probleme verantwortlich. In diesem Fall können Sie mit der Analyse der Untersuchungsaufgaben vom Typ ContainerScan und ODS fortfahren.

6. Deaktivieren Sie die Erstellung von Ablaufverfolgungsdateien der App, indem Sie den folgenden Befehl ausführen:

```
kesl-control --set-app-settings TraceLevel=None
```

7. Ermitteln Sie, welche Objekte am häufigsten untersucht wurden, indem Sie den folgenden Befehl ausführen:

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | sort | uniq -c | sort -k1 -n -r|less
```

Das Ergebnis wird in der App zum Betrachten von Textdateien "less" angezeigt, wobei die Objekte, die am häufigsten untersucht wurden, ganz am Anfang stehen.

8. Stellen Sie fest, ob die am häufigsten untersuchten Objekte gefährlich sind. Bei Problemen wenden Sie sich an den Technischen Support.

Als ungefährlich können Sie zum Beispiel Verzeichnisse und Protokolldateien kennzeichnen, sofern ein vertrauenswürdiger Prozess in diese schreibt, oder Datenbankdateien.

9. Notieren Sie sich die Pfade zu den Objekten, die Ihrer Meinung nach ungefährlich sind – Sie werden sie später benötigen, um Ausschlüsse von der Untersuchung zu konfigurieren.

10. Wenn mehrere Dienste im System häufig in Dateien schreiben, werden solche Dateien wiederholt in einer verzögerten Warteschlange untersucht. Ermitteln Sie, welche Pfade am häufigsten in einer verzögerten Warteschlange untersucht wurden, indem Sie den folgenden Befehl ausführen:

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $9}' | sort | uniq -c | sort -k1 -n -r
```

Die Dateien, die am häufigsten untersucht wurden, werden am Anfang der Liste angezeigt.

11. Wenn der Zähler für eine einzelne Datei in wenigen Stunden einen Wert von mehreren Tausend Untersuchungen überschreitet, müssen Sie feststellen, ob Sie dieser Datei vertrauen können, um sie von der Untersuchung ausschließen zu können.

    Diese Entscheidung unterliegt der gleichen Logik wie die vorangehende (s. Punkt 8): Protokolldateien können als ungefährlich eingestuft werden, da sie nicht ausgeführt werden können.

12. Selbst wenn einige Dateien von der Untersuchung des Echtzeitschutzes ausgenommen sind, können sie dennoch von der App abgefangen werden. Sollte mit dem Ausschließen bestimmter Dateien aus dem Echtzeitschutz keine spürbare Leistungssteigerung einhergehen, können Sie den Mountpunkt, in dem sich diese Dateien befinden, komplett vom Abfangen ausschließen. Gehen Sie dazu folgendermaßen vor:

    a. Rufen Sie die Liste mit vom App abgefangen Dateien ab, indem Sie den folgenden Befehl ausführen:

    ```
    grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | sort |
    uniq -c | sort -k1 -n -r
    ```

    b. Verwenden Sie die abgerufene Liste zum Identifizieren der Pfade, in denen eine große Anzahl abgefangener Dateioperationen registriert wurde, und schließen Sie diese vom Abfangen aus.

Analyse der Ausführung der Aufgaben zur Untersuchung auf Befehl

Der hohe Ressourcenverbrauch kann auch durch die Verwendung von Aufgaben vom Typ ODS und ContainerScan verursacht werden. Beachten Sie die folgenden Empfehlungen zur Verwendung von Aufgaben vom Typ ODS:

- Stellen Sie sicher, dass nicht mehrere Aufgaben zur Untersuchung auf Befehl gleichzeitig gestartet werden. Die App ermöglicht den Betrieb in einem solchen Modus, wobei der Ressourcenverbrauch jedoch stark ansteigen kann. Überprüfen Sie den Zeitplan aller Aufgaben vom Typ ODS und ContainerScan (wie beschrieben für die Aufgabe zum Schutz vor bedrohlichen Dateien) lokal oder über Kaspersky Security Center.
- Starten Sie die Untersuchung zum Zeitpunkt der geringsten Serverauslastung.
- Stellen Sie sicher, dass sich unter dem angegebenen Untersuchungspfad keine gemounteten Remote-Ressourcen (SMB/NFS) befinden. Wenn es sich bei der Aufgabe um die Untersuchung einer Remote-Ressource handelt und diese Aufgabe nicht direkt auf dem Server ausgeführt werden kann, der die Ressource bereitstellt, führen Sie die Untersuchung nicht auf Servern mit kritischen Diensten durch, da die Ausführung einer solchen Aufgabe recht viel Zeit in Anspruch nehmen kann (abhängig von der Verbindungsgeschwindigkeit und der Anzahl der Dateien).
- Optimieren Sie die Einstellungen der Aufgabe zur Untersuchung auf Befehl vor ihrem Start.

Aufgabe zum Schutz vor bedrohlichen Dateien konfigurieren

Wenn Sie nach der Analyse der Ausführung der Aufgabe zum Schutz vor bedrohlichen Dateien eine Liste von Verzeichnissen und Dateien erstellt haben, die von der Überprüfung der Aufgabe ausgeschlossen werden können, müssen Sie sie zu den Ausschlüssen hinzufügen.

Ausschlüsse von der Untersuchung

Um das Verzeichnis /tmp/logs und alle Unterverzeichnisse und Dateien rekursiv auszuschließen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

Um eine bestimmte Datei oder Dateien nach Maske im Verzeichnis /tmp/logs auszuschließen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

Um alle Dateien mit der Erweiterung .log im Verzeichnis /tmp/ und in den Unterverzeichnissen rekursiv anhand einer Maske auszuschließen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

Ausschlüsse vom Abfangen

Wenn Sie Dateien eines bestimmten Verzeichnisses nicht nur von der Untersuchung, sondern auch vom Abfangen ausschließen möchten, können Sie den gesamten Mountpunkt ausschließen.

So schließen Sie den gesamten Mountpunkt aus:

1. Wenn das Verzeichnis kein Mountpunkt ist, müssen Sie einen Mountpunkt daraus erstellen. Um beispielsweise einen Mountpunkt aus dem Verzeichnis /tmp zu erstellen, führen Sie den folgenden Befehl aus:

   ```
   mount --bind /tmp/ /tmp
   ```

2. Tragen Sie in die Datei /etc/fstab die folgende Zeile ein, damit der Mountpunkt nach dem Neustart des Servers erhalten bleibt:

   ```
   /tmp /tmp none defaults,bind 0 0
   ```

3. Fügen Sie das Verzeichnis /tmp zu den globalen Ausschlüssen hinzu, indem Sie den folgenden Befehl ausführen:

   ```
   kesl-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
   ```

4. Wenn Sie mehrere Verzeichnisse hinzufügen möchten, erhöhen Sie den Zähler item_0000 jeweils um eine Einheit (item_0001, item_0002 usw.).

Es wird empfohlen, einen Mountpunkt auch dann auszuschließen, wenn es sich dabei um eine gemountete Remote-Ressource mit einer instabilen oder langsamen Verbindung handelt.

Untersuchungstyp ändern

Standardmäßig kann die Aufgabe zum Schutz vor bedrohlichen Dateien die Dateien beim Öffnen und Schließen untersuchen. Wenn bei der Analyse der Ausführung der Aufgabe zum Schutz vor bedrohlichen Dateien zu viele geschriebene Dateien ermittelt wurden, können Sie die Aufgabe so ändern, dass sie nur beim Öffnen der Dateien aktiviert wird. Führen Sie dazu den folgenden Befehl aus:

```
kesl-control --set-set 1 ScanByAccessType=Open
```

In diesem Modus werden Änderungen, die nach dem Öffnen an der Datei vorgenommen wurden, erst nach dem nächsten Zugriff auf die Datei untersucht.

Aufgabe zur Untersuchung auf Befehl konfigurieren

Ausschlüsse von der Untersuchung

Für Aufgaben zur Untersuchung auf Befehl vom Typ ODS und ContainerScan können Sie Ausschlüsse von der Untersuchung konfigurieren. Die Konfiguration erfolgt analog zur Konfiguration von Untersuchungsausnahmen für die Aufgabe zum Schutz vor bedrohlichen Dateien.

Die Einstellungen für Ausschlüsse aus der Untersuchung von einer Aufgabe zur Untersuchung wirkt sich nicht auf Aufgaben zur Untersuchung aus. Sie müssen für jede Aufgabe zur Untersuchung eigene Ausnahmen konfigurieren.

Begrenzung des Speicherverbrauchs für das Entpacken von Archiven

Bei der rekursiven Untersuchung entpackt die Aufgabe zur Untersuchung auf Befehl während der Untersuchung von Archiven diese unter Verwendung von Arbeitsspeicher. Standardmäßig gilt für die App eine Begrenzung in Höhe von 40 % des gesamten verfügbaren Arbeitsspeichers, jedoch mindestens 2 GB. Wenn Ihr System also über mehr als 5 GB Arbeitsspeicher verfügt, können Sie die Speicherauslastung manuell begrenzen. Dies gilt insbesondere für Server mit Hunderten von Gigabyte Arbeitsspeicher.

Begrenzung des Speicherverbrauchs der App festlegen

Sie können die Menge an Arbeitsspeicher begrenzen, die Kaspersky Endpoint Security bei der Durchführung von Untersuchungsaufgaben der Typen OAS, ODS und ContainerScan verwendet.

Standardmäßig nutzt die App nicht mehr als 40 % des gesamten verfügbaren Arbeitsspeichers. Bei Systemen mit viel Arbeitsspeicher (mehr als 5 GB) kann eine Begrenzung der Speichernutzung sinnvoll sein.

Sie können die von der App bei der Untersuchung von Dateien verwendete Größe des Arbeitsspeichers steuern, indem Sie den Parameter `ScanMemoryLimit` in der Konfigurationsdatei kesl.ini verwenden. Der Standardwert des Parameters beträgt 8192 MB.

Der Parameter begrenzt nur die Speichergröße, die bei der Untersuchung von Dateien verwendet wird. Das bedeutet, dass die Gesamtgröße des von der App genutzten Speichers höher sein kann, als der durch diesen Parameter angegebene Wert.

So legen Sie den maximalen Speicherverbrauch für die Untersuchung von Dateien fest:

1. Beenden Sie Kaspersky Endpoint Security.
2. Öffnen Sie die Datei /var/opt/kaspersky/kesl/common/kesl.ini zur Bearbeitung.
3. Im Abschnitt **[General]**: Geben Sie die erforderliche Größe des Arbeitsspeichers im Wert des Parameters `ScanMemoryLimit` an:

   ```
   ScanMemoryLimit=< Größe des Speichers in Megabyte >
   ```

Der Mindestwert für die Einstellung beträgt 2048 MB. Wenn Sie einen Wert unter 2048 MB angeben, verwendet die App den Mindestwert.

Wenn Sie einen Wert angeben, der größer als die Größe des Arbeitsspeichers des Systems ist, verwendet die App bis zu 40 % des gesamten verfügbaren Arbeitsspeichers.

4. Starten Sie Kaspersky Endpoint Security.

Die Begrenzung des Speicherverbrauchs für die Untersuchung von Dateien wird beim Neustart der App geändert.

Anhang 2. Befehle zur Verwaltung von Kaspersky Endpoint Security

Kaspersky Endpoint Security wird über die Befehlszeile mithilfe der Verwaltungsbefehle für Kaspersky Endpoint Security verwaltet.

Sie können die Hilfe zu Verwaltungsbefehlen mit dem folgenden Befehl anzeigen:

```
kesl-control --help <Präfix der Befehlsgruppe>
```

wobei `<Präfix der Befehlsgruppe>` die folgenden Werte annehmen kann:

- -A – Befehle zur Verwaltung der App-Kontrolle
- -B – Befehle zur Backup-Verwaltung
- -C – Befehle zur Verwaltung der allgemeinen Einstellungen für die Untersuchung von Containern
- -D – Befehle zur Verwaltung der Gerätekontrolle
- -E – Befehle zur Verwaltung der Ereignisse der App
- -F – Befehle zur Firewall-Verwaltung
- -H – Befehle zur Verwaltung blockierter Geräte
- -L – Befehle zur Verwaltung der Lizenzschlüssel
- -N – Befehle zur Verwaltung der Einstellungen für die Untersuchung geschützter Verbindungen
- -R – Befehle zur Verwaltung der Integrationsparameter der App Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response (KATA) und mit Kaspersky Endpoint Detection and Response Optimum.
- -S – Befehle der Statistik
- -T – Befehle zur Verwaltung der Aufgaben und Einstellungen der App
- -U – Befehle zur Verwaltung von Benutzern und Benutzerrollen
- -V – Befehle der App im Light Agent-Modus zum Schutz virtueller Umgebungen
- -W – Befehle zur Ausgabe von Ereignissen

Befehle zur Verwaltung der Einstellungen und Aufgaben der App

-T – Präfix, das angibt, dass der Befehl zur Gruppe von Befehlen zur Verwaltung der Einstellungen und Aufgaben der App gehört.

-C – Präfix, das angibt, dass der Befehl zur Gruppe von Befehlen zur Verwaltung der Einstellungen für die Untersuchung von Containern gehört.

-N – Präfix, das angibt, dass der Befehl zur Gruppe von Befehlen zur Verwaltung der Einstellungen für die Untersuchung geschützter Verbindungen gehört.

Befehl kesl-control --export-settings

Mit diesem Befehl können Sie alle App-Einstellungen in die Konsole ausgeben oder in eine Konfigurationsdatei exportieren (einschließlich der allgemeinen Einstellungen für die Untersuchung von Containern, der Einstellungen für die Untersuchung geschützter Verbindungen, der allgemeinen App-Einstellungen und der Aufgabeneinstellungen).

Befehlssyntax

```
kesl-control [-T] --export-settings [--file <Pfad der Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, in der die App-Einstellungen gespeichert werden.

`--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Befehl kesl-control --import-settings

Mit diesem Befehl können Sie alle App-Einstellungen aus der Konfigurationsdatei importieren (einschließlich der allgemeinen Einstellungen für die Untersuchung von Containern, der Einstellungen für die Untersuchung geschützter Verbindungen, der allgemeinen App-Einstellungen und der Aufgabeneinstellungen).

Befehlssyntax

```
kesl-control [-T] --import-settings --file <Pfad der Konfigurationsdatei> [--json]
```

Argumente und Schlüssel

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die Parameter in die App importiert werden.

`--json` – Importiert die Einstellungen aus einer Konfigurationsdatei im JSON-Format. Wenn Sie den Schalter `--json` nicht angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Befehl kesl-control --update-application

Mit diesem Befehl können Sie das heruntergeladene Update der App-Module installieren.

Der Befehl kann nur ausgeführt werden, wenn die App im Standard-Modus verwendet wird.

Befehlssyntax

```
kesl-control [-T] --update-application
```

Befehle zur Verwaltung der allgemeinen App-Einstellungen

Befehl kesl-control --get-app-settings

Mit diesem Befehl können Sie die aktuellen Werte der allgemeinen App-Einstellungen in die Konsole oder in eine Konfigurationsdatei ausgeben.

Befehlssyntax

```
kesl-control [-T] --get-app-settings [--file <Pfad der Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`--file <Pfad der Konfigurationsdatei>` – Pfad der Konfigurationsdatei, in der die allgemeinen App-Einstellungen ausgegeben werden. Wenn Sie den Schalter `--file` nicht angeben, werden die Einstellungen in die Konsole ausgegeben.

Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.

`--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Befehl kesl-control --set-app-settings

Mit diesem Befehl können Sie die Werte der allgemeinen App-Einstellungen mithilfe von Befehlsschaltern oder durch Importieren von Einstellungen aus einer angegebenen Konfigurationsdatei festlegen.

Befehlssyntax

So legen Sie Einstellungen mithilfe von Befehlsschaltern fest:

```
kesl-control [-T] --set-app-settings <Name der Einstellung>=<Wert der Einstellung>
[<Name der Einstellung>=<Wert der Einstellung>]
```

So legen Sie Einstellungen mithilfe einer Konfigurationsdatei fest:

```
kesl-control [-T] --set-app-settings --file <Pfad zur Konfigurationsdatei> [--json]
```

Argumente und Schlüssel

`<Name der Einstellung>=<Wert der Einstellung>` – Name und Wert einer der allgemeinen App-Einstellungen.

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die Parameter in die App importiert werden.

`--json` – Importiert die Einstellungen aus einer Konfigurationsdatei im JSON-Format in die App. Wenn Sie den Schalter `--json` nicht angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Befehle zur Verwaltung der Aufgabeneinstellungen

Befehl kesl-control --get-settings

Mit diesem Befehl können Sie die aktuellen Werte der Einstellungen der angegebenen Aufgabe in die Konsole oder in eine Konfigurationsdatei ausgeben.

Befehlssyntax

```
kesl-control [-T] --get-settings <ID/Name der Aufgabe> [--file <Pfad der Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`--file <Pfad der Konfigurationsdatei>` – Pfad der Konfigurationsdatei, in der die App-Einstellungen ausgegeben werden. Wenn Sie den Schalter `--file` nicht angeben, werden die Einstellungen in die Konsole ausgegeben.

Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.

`--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Befehl kesl-control --set-settings

Mit diesem Befehl können Sie die Werte der Einstellungen der angegebenen Aufgabe mithilfe von Befehlsschaltern oder durch Importieren von Einstellungen aus einer angegebenen Konfigurationsdatei festlegen.

Befehlssyntax

So legen Sie Einstellungen mithilfe von Befehlsschaltern fest:

```
kesl-control [-T] --set-settings <ID/Name der Aufgabe> <Name der Einstellung>=<Wert der Einstellung> [<Name der Einstellung>=<Wert der Einstellung>] [--add-path <Pfad>] [--del-path <Pfad>] [--add-exclusion <Pfad>] [--del-exclusion <Pfad>]
```

So legen Sie Einstellungen mithilfe einer Konfigurationsdatei fest:

```
kesl-control [-T] --set-settings <ID/Name der Aufgabe> --file <Pfad der
Konfigurationsdatei> [--json]
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`<Name der Einstellung>=<Wert der Einstellung>` – Name und Wert einer der Aufgabeneinstellungen.

`--add-path <Pfad>` – Fügen Sie den Pfad zum Verzeichnis mit den untersuchten Objekten hinzu.

`--del-path <Pfad>` – Löscht den Pfad zum Verzeichnis mit den untersuchten Objekten.

`--add-exclusion <Pfad>` – Fügen Sie den Pfad zum Verzeichnis mit den Objekten hinzu, die von der Untersuchung ausgeschlossen werden sollen.

`--del-path <Pfad>` – Löscht den Pfad zum Verzeichnis mit den ausgeschlossenen Objekten.

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die Einstellungen der Aufgabe importiert werden.

`--json` – Importiert die Einstellungen aus einer Konfigurationsdatei im JSON-Format. Wenn Sie den Schalter `--json` nicht angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Befehl kesl-control --set-to-default

Mit diesem Befehl können Sie die Standardwerte der Einstellungen der angegebenen Aufgabe wiederherstellen.

Befehlssyntax

```
kesl-control [-T] --set-settings <ID/Name der Aufgabe> --set-to-default
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Befehl kesl-control --get-schedule

Mit diesem Befehl können Sie den aktuellen Zeitplan für den Start der angegebenen Aufgabe in die Konsole oder in eine Konfigurationsdatei ausgeben.

Befehlssyntax

```
kesl-control [-T] --get-schedule <ID/Name der Aufgabe> [--file <Pfad der
Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`--file <Pfad der Konfigurationsdatei>` – Pfad der Konfigurationsdatei, in der die Einstellungen für den Aufgabenzeitplan ausgegeben werden. Wenn Sie den Schalter `--file` nicht angeben, werden die Einstellungen in die Konsole ausgegeben.

Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.

`--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Befehl kesl-control --set-schedule

Mit diesem Befehl können Sie den Zeitplan der angegebenen Aufgabe mithilfe von Befehlsschaltern oder durch Importieren von Einstellungen aus einer angegebenen Konfigurationsdatei festlegen.

Befehlssyntax

So legen Sie Einstellungen mithilfe von Befehlsschaltern fest:

```
kesl-control [-T] --set-schedule <ID/Name der Aufgabe> <Name der Einstellung>=<Wert der Einstellung> [<Name der Einstellung>=<Wert der Einstellung>]
```

So legen Sie Einstellungen mithilfe einer Konfigurationsdatei fest:

```
kesl-control [-T] --set-schedule <ID/Name der Aufgabe> --file <Pfad der Konfigurationsdatei> [--json]
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`<Name der Einstellung>=<Wert der Einstellung>` – Name und Wert einer der Einstellungen des Aufgabenzeitplans.

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die Einstellungen des Aufgabenzeitplans importiert werden.

`--json` – Importiert die Einstellungen aus einer Konfigurationsdatei im JSON-Format. Wenn Sie den Schalter `--json` nicht angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Befehle zur Aufgabenverwaltung

Befehl kesl-control --get-task-list

Mit diesem Befehl können Sie die Liste der vorhandenen App-Aufgaben anzeigen.

Befehlssyntax

```
kesl-control [-T] --get-task-list [--json]
```

Argumente und Schlüssel

`--json` – Gibt die Einstellungen im JSON-Format aus.

Befehl kesl-control --get-task-state

Mit diesem Befehl können Sie den Status der angegebenen Aufgabe ausgeben.

Befehlssyntax

```
kesl-control [-T] --get-task-state <ID/Name der Aufgabe> [--json]
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`--json` – Gibt die Einstellungen im JSON-Format aus.

Befehl kesl-control --create-task

Mit diesem Befehl können Sie eine Aufgabe des angegebenen Typs mit Standardeinstellungen oder mit den in der Konfigurationsdatei angegebenen Einstellungen erstellen.

Befehlssyntax

So erstellen Sie eine Aufgabe mit Standardeinstellungen:

```
kesl-control [-T] --create-task <Aufgabenname> --type <Aufgabentyp>
```

So erstellen Sie eine Aufgabe mit Einstellungen aus der Konfigurationsdatei:

```
kesl-control [-T] --create-task <Aufgabenname> --type <Aufgabentyp> [--file <Pfad der Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`<Aufgabenname>` – Name, den Sie für eine neue Aufgabe vergeben.

`<Aufgabentyp>` – Bezeichnung des Typs der zu erstellenden Aufgabe.

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, deren Einstellungen beim Erstellen der Aufgabe verwendet werden.

`--json` – Importiert die Einstellungen aus einer Konfigurationsdatei im JSON-Format. Wenn Sie den Schalter `--json` nicht angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Befehl kesl-control --delete-task

Mit diesem Befehl können Sie eine Aufgabe löschen.

Befehlssyntax

```
kesl-control [-T] --delete-task <ID/Name der Aufgabe>
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Befehl kesl-control --start-task

Mit diesem Befehl können Sie eine Aufgabe starten.

Befehlssyntax

```
kesl-control [-T] --start-task <ID/Name der Aufgabe> [-W] [--progress]
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`[-W]` – Ausgabe aktueller Ereignisse aktivieren.

`[--progress]` – Fortschritt der laufenden Aufgabe anzeigen.

Befehl kesl-control --stop-task

Mit diesem Befehl können Sie die Aufgabe beenden.

Befehlssyntax

```
kesl-control [-T] --stop-task <ID/Name der Aufgabe> [-W]
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`[-W]` – Ausgabe aktueller Ereignisse aktivieren.

Befehl kesl-control --suspend-task

Mit diesem Befehl können Sie eine Aufgabe anhalten.

Befehlssyntax

```
kesl-control [-T] --suspend-task <ID/Name der Aufgabe>
```

Argumente und Schlüssel

< ID/Name der Aufgabe > – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Befehl kesl-control --resume-task

Mit diesem Befehl können Sie die Ausführung der Aufgabe fortsetzen.

Befehlssyntax

```
kesl-control [-T] --resume-task < ID/Name der Aufgabe >
```

Argumente und Schlüssel

< ID/Name der Aufgabe > – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Befehl kesl-control --scan-file

Mit diesem Befehl können Sie eine Aufgabe zur benutzerdefinierten Untersuchung erstellen und starten.

Befehlssyntax

```
kesl-control [-T] --scan-file < Pfad > [--action < Aktion >]
```

Argumente und Schlüssel

< Pfad > – Pfad der Datei oder des Verzeichnisses, die bzw. das Sie untersuchen möchten. Sie können mehrere, durch Leerzeichen getrennte Pfade angeben.

--action < Aktion > – Aktion, welche die App für infizierte Objekte ausführen soll. Wenn Sie den Schalter --action nicht angeben, führt die App die empfohlene Aktion aus.

Befehl kesl-control --scan-container

Mit diesem Befehl können Sie eine Aufgabe zur benutzerdefinierten Untersuchung für einen Container oder ein Image erstellen und starten.

Befehlssyntax

```
kesl-control [-T] --scan-container < Container/Image [: Tag ]>
```

Argumente und Schlüssel

< Container/Image [: Tag]> – Name oder ID des Containers oder Images. Bei der Untersuchung mehrerer Objekte können Masken verwendet werden.

Verwenden Sie das Zeichen * (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen / im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne * verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske ** kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Sie können das Symbol ? anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Befehle zur Verwaltung der allgemeinen Einstellungen für die Untersuchung von Containern

Befehl kesl-control --get-container-settings

Mit diesem Befehl können Sie die aktuellen Werte der allgemeinen Einstellungen für die Untersuchung von Containern in die Konsole oder in eine Konfigurationsdatei ausgeben.

Befehlssyntax

```
kesl-control [-C] --get-container-settings [--file <Pfad der Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`--file <Pfad der Konfigurationsdatei>` – Pfad der Konfigurationsdatei, in die die allgemeinen Einstellungen für die Untersuchung von Containern ausgegeben werden. Wenn Sie den Schalter `--file` nicht angeben, werden die Einstellungen in die Konsole ausgegeben.

Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.

`--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Befehl kesl-control --set-container-settings

Mit diesem Befehl können Sie die Werte der allgemeinen Einstellungen für die Container-Untersuchung mithilfe von Befehlsschaltern oder durch Importieren von Einstellungen aus einer angegebenen Konfigurationsdatei festlegen.

Befehlssyntax

So legen Sie Einstellungen mithilfe von Befehlsschaltern fest:

```
kesl-control [-C] --set-container-settings <Name der Einstellung>=<Wert der Einstellung>
[<Name der Einstellung>=<Wert der Einstellung>]
```

So legen Sie Einstellungen mithilfe einer Konfigurationsdatei fest:

```
kesl-control [-C] --set-container-settings --file <Pfad der Konfigurationsdatei> [--
json]
```

Argumente und Schlüssel

`<Name der Einstellung>=<Wert der Einstellung>` – Name und Wert einer der allgemeinen Einstellungen für die Container-Untersuchung.

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die allgemeinen Einstellungen für die Container-Untersuchung importiert werden.

`--json` – Importiert die Einstellungen aus einer Konfigurationsdatei im JSON-Format in die App. Wenn Sie den Schalter `--json` nicht angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Befehle zur Verwaltung der Einstellungen für die Untersuchung geschützter Verbindungen

-N – Präfix, das angibt, dass der Befehl zur Gruppe von Befehlen zur Verwaltung der Einstellungen für die Untersuchung geschützter Verbindungen gehört.

Befehl kesl-control -N --query

Mit diesem Befehl können Sie Listen mit Ausschlüssen von der Untersuchung geschützter Verbindungen ausgeben:

- Liste der vom Benutzer hinzugefügten Ausschlüsse;
- Liste der von der App hinzugefügten Ausschlüsse;
- Liste der von den App-Datenbanken abgerufenen Ausschlüsse.

Befehlssyntax

```
kesl-control -N --query user

kesl-control -N --query auto

kesl-control -N --query kl
```

Befehl kesl-control --clear-web-auto-excluded

Mit diesem Befehl können Sie die Liste der Domänen löschen, die die App automatisch von der Untersuchung ausgeschlossen hat.

Befehlssyntax

```
kesl-control -N --clear-web-auto-excluded
```

Befehl kesl-control --get-net-settings

Mit diesem Befehl können Sie die aktuellen Werte der Einstellungen für die Untersuchung geschützter Verbindungen in die Konsole oder in eine Konfigurationsdatei ausgeben.

Befehlssyntax

```
kesl-control [-N] --get-net-settings [--file <Pfad der Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`--file <Pfad der Konfigurationsdatei>` – Pfad der Konfigurationsdatei, in die die Einstellungen für die Untersuchung geschützter Verbindungen ausgegeben werden. Wenn Sie den Schalter `--file` nicht angeben, werden die Einstellungen in die Konsole ausgegeben.

Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.

`--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Befehl kesl-control --set-net-settings

Mit diesem Befehl können Sie die Werte der Einstellungen für die Untersuchung geschützter Verbindungen mithilfe von Befehlsschaltern oder durch Importieren von Einstellungen aus einer angegebenen Konfigurationsdatei festlegen.

Befehlssyntax

So legen Sie Einstellungen mithilfe von Befehlsschaltern fest:

```
kesl-control [-N] --set-net-settings <Name der Einstellung>=<Wert der Einstellung>
[<Name der Einstellung>=<Wert der Einstellung>]
```

So legen Sie Einstellungen mithilfe einer Konfigurationsdatei fest:

```
kesl-control [-N] --set-net-settings --file <Pfad der Konfigurationsdatei> [--json]
```

Argumente und Schlüssel

`<Name der Einstellung>=<Wert der Einstellung>` – Name und Wert einer der Einstellungen zur Untersuchung geschützter Verbindungen.

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die Einstellungen für die Untersuchung geschützter Verbindungen importiert werden.

`--json` – Importiert die Einstellungen aus einer Konfigurationsdatei im JSON-Format in die App. Wenn Sie den Schalter `--json` nicht angeben, versucht die App, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Befehl kesl-control --add-certificate

Mit diesem Befehl können Sie ein Zertifikat zur Liste der Zertifikate hinzufügen, die die App als vertrauenswürdig erachten soll.

Befehlssyntax

```
kesl-control [-N] -add-certificate <Pfad des Zertifikats>
```

Argumente und Schlüssel

`<Pfad des Zertifikats>` – Pfad der Zertifikatsdatei, die Sie hinzufügen möchten, im PEM- oder DER-Format.

Befehl kesl-control --remove-certificate

Mit diesem Befehl können Sie ein Zertifikat aus der Liste der vertrauenswürdigen Zertifikate entfernen.

Befehlssyntax

```
kesl-control [-N] --remove-certificate <Zertifikatinhaber>
```

Befehl kesl-control --list-certificates

Mit diesem Befehl können Sie die Liste vertrauenswürdiger Zertifikate ausgeben.

Befehlssyntax

```
kesl-control [-N] --list-certificates
```

Statistikbefehle

-S – Präfix, das angibt, dass der Befehl zur Gruppe der Statistikbefehle gehört.

Befehl kesl-control --app-info

Mit diesem Befehl können Sie Informationen zur App ausgeben.

Befehlssyntax

```
kesl-control [-S] --app-info [--json]
```

Argumente und Schlüssel

`--json` – Gibt die Einstellungen im JSON-Format aus.

Befehl kesl-control --omsinfo

Mit diesem Befehl können Sie eine Datei im JSON-Format für die Integration mit der Microsoft Operations Management Suite erstellen.

Befehlssyntax

```
kesl-control [-S] --omsinfo --file <Dateiname und Dateipfad>
```

Befehle zur Anzeige von Ereignissen

Befehl kesl-control -W

Der Befehl aktiviert die Ausgabe aktueller App-Ereignisse. Der Befehl gibt den Namen des Ereignisses und zusätzliche Informationen über das Ereignis zurück. Mit diesem Befehl können Sie alle aktuellen App-Ereignisse oder nur Ereignisse ausgeben, die mit der ausgeführten Aufgabe verknüpft sind.

Befehlssyntax

```
kesl-control -W [--query "<Filterbedingungen>"]
```

Argumente und Schlüssel

`<Filterbedingungen>` – Ein oder mehrere logische Ausdrücke im Format `<Feld> <Vergleichsoperator> '<Wert>'`, kombiniert mit dem logischen Operator `and` zur Ausgabe bestimmter aktueller Ereignisse.

Befehle zur Verwaltung der App-Ereignisse

-E – Präfix, das angibt, dass der Befehl zur Gruppe der Befehle zur Verwaltung der App-Ereignisse gehört.

Befehl kesl-control -E

Mit diesem Befehl können Sie Informationen zu allen Ereignissen aus dem Ereignisprotokoll der App ausgeben. Mit dem Tool `less` können Sie durch die Liste der angezeigten Ereignisse navigieren.

Befehlssyntax

```
kesl-control -E
```

Befehl kesl-control -E --query

Mit diesem Befehl können Sie Informationen zu Ereignissen aus dem Ereignisprotokoll der App ausgeben. Mit dem Tool `less` können Sie durch die Liste der angezeigten Ereignisse navigieren. Sie können einen Filter verwenden, um bestimmte Ereignisse auszugeben und auch eine Liste von Ereignissen in eine bestimmte Datei auszugeben.

Befehlssyntax

```
kesl-control -E --query "<Filterbedingungen>" [--db <Datenbankdatei>] [-n <Anzahl>] [--file <Dateiname und Dateipfad>] [--json] [--reverse]
```

Argumente und Schlüssel

< Datenbankdatei > – Vollständiger Pfad zur Datenbankdatei des Ereignisprotokolls, aus dem Sie Ereignisse ausgeben möchten. Standardmäßig speichert die App die Informationen über Ereignisse in der Datenbank /var/opt/kaspersky/kesl/private/storage/events.db. Der Speicherort der Datenbank wird durch die allgemeine App-Einstellung `EventsStoragePath` bestimmt.

< Filterbedingungen > – Ein oder mehrere logische Ausdrücke im Format < Feld > < Vergleichsoperator > '< Wert >', kombiniert mit dem logischen Operator `and` zur Eingrenzung der Abfrageergebnisse.

< Anzahl > – Anzahl der letzten Ereignisse aus der Auswahl (d. h. die Anzahl der Einträge ab Ende der Auswahl), die ausgegeben werden sollen.

`--file` < Dateiname und Dateipfad > – Vollständiger Pfad zu der Datei, in die Sie die Ereignisse ausgeben möchten. Wenn Sie den Dateinamen eingeben, ohne einen Dateipfad vorzugeben, wird die Datei im aktuellen Verzeichnis erstellt. Ist unter dem gewünschten Pfad bereits eine Datei mit gleichem Namen vorhanden, wird diese überschreiben. Falls das von Ihnen vorgegebene Verzeichnis auf der Festplatte nicht existiert, wird die Datei nicht erstellt.

Wenn Sie den Schalter `--file` nicht angeben, wir die Liste der Ereignisse in die Konsole ausgegeben.

`--json` – Gibt die Ereignisse im JSON-Format aus.

`--reverse` – Ereignisse in umgekehrter Reihenfolge anzeigen (das neueste Ereignis steht oben und das ältesten unten).

Befehle zur Verwaltung der Lizenzschlüssel

-L – Präfix, das angibt, dass der Befehl zur Gruppe der Befehle zur Verwaltung von Lizenzschlüsseln gehört

> Die Befehle zum Hinzufügen und Entfernen von Lizenzschlüsseln können nur ausgeführt werden, wenn die App im Standard-Modus verwendet wird. Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, schlagen die Befehle zur Verwaltung von Lizenzschlüsseln mit einem Fehler fehl. Sie aktivieren die App als Teil der Lösung Kaspersky Security for Virtualization Light Agent; Sie müssen die App nicht separat aktivieren.

Befehl kesl-control --add-active-key

Mit diesem Befehl können Sie der App mithilfe einer Schlüsseldatei oder eines Aktivierungscodes einen aktiven Lizenzschlüssel hinzufügen.

Mit diesem Befehl können Sie sowohl aktive Lizenzschlüssel für die App als auch für EDR Optimum hinzufügen. Der Schlüsseltyp muss nicht im Befehl angeben werden.

Befehlssyntax

```
kesl-control [-L] --add-active-key < Pfad der Schlüsseldatei >

kesl-control [-L] --add-active-key < Aktivierungscode >
```

Argumente und Schlüssel

< Pfad zur Schlüsseldatei > – Pfad zur Schlüsseldatei. Wenn sich die Schlüsseldatei im aktuellen Verzeichnis befindet, ist die Angabe des Dateinamens ausreichend.

< Aktivierungscode > – Aktivierungscode.

Beispiel:
So fügen Sie einen Schlüssel mithilfe der Datei /home/test/00000001.key als aktiven Schlüssel hinzu:

```
kesl-control --add-active-key /home/test/00000001.key
```

Befehl kesl-control --add-reserve-key

Mit diesem Befehl können Sie mithilfe einer Schlüsseldatei oder eines Aktivierungscodes einen Reserve-Lizenzschlüssel zur App hinzufügen.

Mit diesem Befehl können Sie sowohl Reserve-Lizenzschlüssel für die App als auch für EDR Optimum hinzufügen. Der Schlüsseltyp muss nicht im Befehl angeben werden.

Wenn der App auf dem Gerät noch kein aktiver Schlüssel hinzugefügt wurde, schlägt der Befehl fehl.

Befehlssyntax

```
kesl-control [-L] --add-reserve-key < Pfad der Schlüsseldatei >

kesl-control [-L] --add-reserve-key < Aktivierungscode >
```

Argumente und Schlüssel

< Pfad zur Schlüsseldatei > – Pfad zur Schlüsseldatei. Wenn sich die Schlüsseldatei im aktuellen Verzeichnis befindet, ist die Angabe des Dateinamens ausreichend.

< Aktivierungscode > – Aktivierungscode.

Beispiel:
So fügen Sie einen Reserveschlüssel mithilfe der Datei /home/test/00000002.key hinzu:

```
kesl-control --add-reserve-key /home/test/00000002.key
```

Befehl kesl-control --remove-active-key

Mit diesem Befehl können Sie einen aktiven Lizenzschlüssel löschen.

Befehlssyntax

```
kesl-control [-L] --remove-active-key [--edr-optimum]
```

Argumente und Schlüssel

`--edr-optimum` – Entfernt den aktiven EDR Optimum-Lizenzschlüssel. Wenn Sie den Schalter `--edr-optimum` nicht angeben, wird stattdessen der aktive Lizenzschlüssel von Kaspersky Endpoint Security gelöscht.

Befehl kesl-control --remove-reserve-key

Mit diesem Befehl können Sie einen Reserve-Lizenzschlüssel löschen.

Befehlssyntax

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

Argumente und Schlüssel

`--edr-optimum` – Entfernt den Reserve-Lizenzschlüssel von EDR Optimum. Wenn Sie den Schalter `--edr-optimum` nicht angeben, wird stattdessen der Reservelizenzschlüssel von Kaspersky Endpoint Security gelöscht.

Befehl kesl-control -L --query

Mit dem Befehl `-L --query` können Sie Informationen über die Lizenz, mit der die App aktiviert wurde, und die verwendeten Lizenzschlüssel ausgeben.

Befehlssyntax

```
kesl-control -L --query [--json]
```

Argumente und Schlüssel

`--json` – Gibt Daten im JSON-Format aus.

Befehl kesl-control --load-mdr-blob

Mit dem Befehl `--load-mdr-blob` können Sie die BLOB-Konfigurationsdatei laden, die für die Integration mit Kaspersky Managed Detection and Response erforderlich ist.

Befehlssyntax

```
kesl-control [-L] --load-mdr-blob <Pfad der Konfigurationsdatei MDR BLOB>
```

Befehl kesl-control --remove-mdr-blob

Mit dem Befehl `--remove-mdr-blob` können Sie die BLOB-Konfigurationsdatei entfernen, die für die Integration mit Kaspersky Managed Detection and Response erforderlich ist.

Befehlssyntax

```
kesl-control [-L] --remove-mdr-blob
```

Befehle zur Firewall-Verwaltung

-F – Präfix, das angibt, dass der Befehl zur Gruppe der Befehle der Firewall-Verwaltung gehört.

Befehl kesl-control --add-rule

Mit diesem Befehl können Sie eine neue Netzwerkpaketregel hinzufügen.

Befehlssyntax

```
kesl-control [-F] --add-rule [--name <Regelname>] [--action <Aktion>] [--protocol
<Protokoll>] [--direction <Richtung>] [--remote <Remote-Adresse>[:<Portbereich>]] [--
local <lokale Adresse>[:<Portbereich>]] [--at <Index>]
```

Argumente und Schlüssel

`--name <Regelname>` – Name der Netzwerkpaketregel.

`--action <Aktion>` – Aktion, die mit den in dieser Netzwerkpaketregel angegebenen Verbindungen ausgeführt wird.

`--protocol <Protokoll>` – Typ des Datenübertragungsprotokolls, für das Sie die Netzwerkaktivität überwachen wollen.

`--direction <Richtung>` – Richtung der überwachten Netzwerkaktivität.

`--remote <Remote-Adresse>[:<Portbereich>]` – Netzwerkadresse des Remote-Geräts.

`--local <lokale Adresse>[:<Portbereich>]` – Netzwerkadresse des Geräts, auf dem Kaspersky Endpoint Security installiert ist.

`--at <Index>` – Fortlaufende Nummer der Regel in der Liste der Netzwerkpaketregeln. Wenn der Schalter `--at` nicht angegeben wird oder sein Wert größer als die Anzahl der Regeln in der Liste ist, wird die neue Regel zum Ende der Liste hinzugefügt.

Einstellungen, für die Sie im Befehl keine Werte angeben, werden auf ihre Standardwerte gesetzt.

Befehl kesl-control --del-rule

Mit diesem Befehl können Sie eine Netzwerkpaketregel mit dem angegebenen Namen oder mit dem angegebenen Index in der Regelliste löschen.

Befehlssyntax

```
kesl-control [-F] --del-rule --name <Regelname>

kesl-control [-F] --del-rule --index <Index>
```

Argumente und Schlüssel

`--name <Regelname>` – Name der Netzwerkpaketregel.

`--index <Index>` – Fortlaufende Nummer der Regel in der Liste der Netzwerkpaketregeln.

Befehl kesl-control --move-rule

Mit diesem Befehl können Sie die Ausführungspriorität einer Netzwerkpaketregel ändern.

Befehlssyntax

```
kesl-control [-F] --move-rule --name <Regelname> --at <Index>
```

```
kesl-control [-F] --move-rule --index <Index> --at <Index>
```

Argumente und Schlüssel

`--name <Regelname>` – Name der Netzwerkpaketregel.

`--index <Index>` – Aktuelle fortlaufende Nummer der Regel in der Liste der Netzwerkpaketregeln.

`--at <Index>` – Neue fortlaufende Nummer der Regel in der Liste der Netzwerkpaketregeln.

Befehl kesl-control --add-zone

Mit diesem Befehl können Sie eine Adresse zu einer Netzwerkzone hinzufügen.

Befehlssyntax

```
kesl-control [-F] --add-zone --zone <Zone> --address <Adresse>
```

Argumente und Schlüssel

`--zone <Zone>` – Vordefinierter Name der Netzwerkzone.

`--address <Adresse>` – Netzwerkadresse oder Subnetz.

Befehl kesl-control --del-zone

Mit diesem Befehl können Sie eine Adresse aus der Netzwerkzone löschen.

Befehlssyntax

```
kesl-control [-F] --del-zone --zone <Zone> --address <Adresse>
```

```
kesl-control [-F] --del-zone --zone <Zone> --index <Adressindex>
```

Argumente und Schlüssel

`--zone <Zone>` – Vordefinierter Name der Netzwerkzone.

`--address <Adresse>` – Netzwerkadresse oder Subnetz.

`--index <Adressindex>` – Fortlaufende Nummer der Adresse in der Netzwerkzone.

Befehl kesl-control -F --query

Mit diesem Befehl können Sie die Firewall-Regeln anzeigen, die mithilfe von Kaspersky Endpoint Security erstellt wurden.

Befehlssyntax

```
kesl-control -F --query
```

Befehle zur Verwaltung blockierter Geräte

-H – Präfix, das angibt, dass der Befehl zur Gruppe der Befehle zur Verwaltung von Geräten gehört, die durch den Schutz vor Verschlüsselung und den Schutz vor Netzwerkbedrohungen gesperrt wurden.

Befehl kesl-control --get-blocked-hosts

Mit diesem Befehl können Sie die Liste der blockierten Geräte in die Konsole ausgeben.

Befehlssyntax

```
kesl-control [-H] --get-blocked-hosts
```

Befehl kesl-control --allow-hosts

Mit diesem Befehl können Sie gesperrte Geräte entsperren.

Befehlssyntax

```
kesl-control [-H] --allow-hosts <Adresse>
```

Argumente und Schlüssel

`<Adresse>` – IP-Adresse des Geräts oder Subnetzes (IPv4/IPv6, einschließlich Adressen in Kurzform). Sie können mehrere, durch Leerzeichen getrennte IP-Adressen von Geräten oder Subnetzen angeben.

Befehle zur Verwaltung der Gerätekontrolle

-D – Präfix, das angibt, dass der Befehl zur Gruppe der Befehle zur Verwaltung der Gerätekontrolle gehört.

Befehl kesl-control --get-device-list

Mit diesem Befehl können Sie die Liste der Geräte, die auf dem Client-Gerät installiert oder mit ihm verbunden sind, in die Konsole ausgeben.

Befehlssyntax

```
kesl-control [-D] --get-device-list [--json]
```

Argumente und Schlüssel

`--json` – Gibt Daten im JSON-Format aus.

Befehle zur Verwaltung der App-Kontrolle

-A – Präfix, das angibt, dass der Befehl zur Gruppe der Befehle für die Verwaltung der App-Kontrolle gehört.

Befehl kesl-control --get-app-list

Mit diesem Befehl können Sie die Liste der Apps ausgeben, die während der Ausführung der Aufgabe "Inventarisierung" auf dem Client-Gerät erkannt wurden.

Befehlssyntax

```
kesl-control [-A] --get-app-list [--json]
```

Argumente und Schlüssel

`--json` – Gibt Daten im JSON-Format aus.

Befehl kesl-control --get-categories

Mit diesem Befehl können Sie die Liste der erstellten Kategorien der App-Kontrolle ausgeben.

Befehlssyntax

```
kesl-control [-A] --get-categories [--names <Kategoriename 1> <Kategoriename 2> ...
<Kategoriename N>] --file [<Pfad zur Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`<Kategoriename 1> <Kategoriename 2> ... <Kategoriename N>` – Namen der Kategorien, deren Informationen Sie anzeigen möchten. Wenn Sie Informationen mehrerer Kategorien anzeigen möchten, geben Sie die Kategorienamen durch ein Leerzeichen getrennt an.

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei im JSON-Format, in der die Einstellungen ausgegeben werden.

`--json` – Gibt Daten im JSON-Format aus.

Befehl kesl-control --set-categories

Mit diesem Befehl können Sie die Liste der erstellten Kategorien der App-Kontrolle erstellen oder ändern.

Befehlssyntax

```
kesl-control [-A] --set-categories [--names <Kategoriename 1> <Kategoriename 2> ...
<Kategoriename N>] --file <Pfad zur Konfigurationsdatei>
```

Argumente und Schlüssel

`<Kategoriename 1> <Kategoriename 2> ... <Kategoriename N>` – Namen der Kategorien, deren Informationen Sie ändern möchten. Wenn Sie Informationen mehrerer Kategorien ändern möchten, geben Sie die Kategorienamen durch ein Leerzeichen getrennt an. Wenn Sie keinen Kategorienamen angeben, wird diese aus der Liste entfernt.

`--file <Pfad zur Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei mit den allgemeinen App-Einstellungen.

Befehl kesl-control --get-settings

Mit diesem Befehl können Sie die Liste der erstellten Regeln der App-Kontrolle ausgeben.

Befehlssyntax

```
kesl-control --get-settings 21 [--file <Pfad zur Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, in der die Einstellungen ausgegeben werden.

`--json` – Gibt Daten im JSON-Format aus.

Befehl kesl-control --set-settings

Mit dem Befehl können Sie die Liste der erstellten App-Kategorien und Regeln der App-Kontrolle ändern.

Befehlssyntax

```
kesl-control --set-settings 21 [--file <Pfad zur Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die Einstellungen importiert werden.

`--json` – Importiert die Daten aus einer Datei im JSON-Format importiert.

Befehl kesl-control --set-to-default

Mit dem Befehl können Sie die Liste der App-Kategorien und Regeln der App-Kontrolle löschen.

Befehlssyntax

```
kesl-control --set-settings 21 --set-to-default
```

Befehle zur Verwaltung der Web-Kontrolle

Befehl kesl-control --get-settings

Mit dem Befehl können Sie eine Liste der konfigurierten Parameter der Web-Kontrolle anzeigen.

Befehlssyntax

```
kesl-control --get-settings 26 [--file <Pfad zur Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, in der die Einstellungen ausgegeben werden.

`--json` – Gibt Daten im JSON-Format aus.

Befehl kesl-control --set-settings

Mit dem Befehl können Sie eine Liste der konfigurierten Parameter der Web-Kontrolle ändern.

Befehlssyntax

```
kesl-control --set-settings 26 [--file <Pfad zur Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die Einstellungen importiert werden.

`--json` – Importiert die Daten aus einer Datei im JSON-Format importiert.

Befehl kesl-control --set-to-default

Mit dem Befehl können Sie die konfigurierten Parameter der Web-Kontrolle löschen und die Werte der Einstellungen auf die Standardregel zurücksetzen.

Befehlssyntax

```
kesl-control --set-settings 26 --set-to-default
```

Befehle zur Backup-Verwaltung

-B – Präfix, das angibt, dass der Befehl zur Gruppe der Befehle zur Verwaltung des Backups gehört.

Befehl kesl-control --mass-remove

Mit diesem Befehl können Sie alle oder nur bestimmte Objekte aus dem Backup löschen.

Befehlssyntax

Alle Objekte löschen:

```
kesl-control [-B] --mass-remove
```

Objekte löschen, die den Filterbedingungen entsprechen:

```
kesl-control [-B] --mass-remove --query "<Filterbedingungen>"
```

Argumente und Schlüssel

`<Filterbedingungen>` – Ein oder mehrere logische Ausdrücke im Format `<Feld> <Vergleichsoperator> '<Wert>'`, kombiniert mit dem logischen Operator `and` zur Eingrenzung der Abfrageergebnisse.

Befehl kesl-control -B --query

Mit diesem Befehl können Sie Informationen zu Backup-Objekten ausgeben.

Befehlssyntax

Informationen zu allen Backup-Objekten ausgeben:

```
kesl-control -B --query [-n <Anzahl>] [--json] [--reverse]
```

Informationen zu Backup-Objekten ausgeben, die den Filterbedingungen entsprechen:

```
kesl-control -B --query ["<Filterbedingungen>"] [-n <Anzahl>] [--json] [--reverse]
```

Argumente und Schlüssel

`<Filterbedingungen>` – Ein oder mehrere logische Ausdrücke im Format `<Feld> <Vergleichsoperator> '<Wert>'`, kombiniert mit dem logischen Operator `and` zur Eingrenzung der Abfrageergebnisse. Wenn Sie keine Filterbedingungen angeben, zeigt die App Informationen zu allen Backup-Objekten an.

`<Anzahl>` – Die Anzahl der letzten Objekte aus dem Backup, die ausgegeben werden müssen. Wenn Sie den Schalter `-n` nicht angeben, werden die letzten 30 Objekte ausgegeben. Um alle Objekte anzuzeigen, geben Sie den Wert 0 ein.

`--json` – Gibt Daten im JSON-Format aus.

Befehl kesl-control --restore

Mit diesem Befehl können Sie ein Objekt aus dem Backup wiederherstellen.

Befehlssyntax

```
kesl-control [-B] --restore <Objekt-ID> [--file <Dateiname und Dateipfad>]
```

Argumente und Schlüssel

`<Objekt-ID>` – ID des Objekts im Backup.

`--file <Dateiname und Dateipfad>` – Der neue Dateiname und der Pfad zu dem Verzeichnis, in dem die Datei gespeichert werden soll. Wenn Sie den Schalter `--file` nicht angeben, wird das Objekt mit seinem ursprünglichen Namen an seinem ursprünglichen Speicherort wiederhergestellt.

Befehle zur Verwaltung von Benutzern und Rollen

-U – Präfix, das angibt, dass der Befehl zur Gruppe von Befehlen zur Verwaltung von Benutzern und Rollen gehört

Befehl kesl-control --get-user-list

Mit diesem Befehl können Sie die Liste der Benutzer und Rollen ausgeben.

Befehlssyntax

```
kesl-control [-U] --get-user-list
```

Befehl kesl-control --grant-role

Mit diesem Befehl können Sie einem bestimmten Benutzer eine Rolle zuweisen.

Befehlssyntax

```
kesl-control [-U] --grant-role <Rolle> <Benutzer>
```

Befehl kesl-control --revoke-role

Mit diesem Befehl können Sie einem bestimmten Benutzer eine Rolle entziehen.

Befehlssyntax

```
kesl-control [-U] --revoke-role <Rolle> <Benutzer>
```

Befehle zur Verwaltung der Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA)

-R – ein Präfix, das angibt, dass der Befehl zur Befehlsgruppe zur Verwaltung der Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA) und mit Kaspersky Endpoint Detection and Response Optimum gehört.

Befehl kesl-control --add-kataedr-server-certificate

Mit diesem Befehl können Sie ein zuvor hinzugefügtes Zertifikat des KATA-Servers hinzufügen oder ersetzen.

Befehlssyntax

```
kesl-control [-R] --add-kataedr-server-certificate <Dateiname und Dateipfad>
```

Argumente und Schlüssel

`<Dateiname und Dateipfad>` – Name und Pfad der Datei, die das Serverzertifikat enthält.

Befehl kesl-control --remove-kataedr-server-certificate

Mit diesem Befehl können Sie das Zertifikat des KATA-Servers löschen.

Befehlssyntax

```
kesl-control [-R] --remove-kataedr-server-certificate
```

Befehl kesl-control --query-kataedr-server-certificate

Mit diesem Befehl können Sie Informationen zum Zertifikat des KATA-Servers anzeigen.

Befehlssyntax

```
kesl-control [-R] --query-kataedr-server-certificate
```

Befehl kesl-control --add-kataedr-client-certificate

Mit diesem Befehl können Sie ein zuvor hinzugefügtes Client-Zertifikat hinzufügen oder ersetzen, das zum Sichern der Verbindung zum KATA-Server verwendet wird.

Befehlssyntax

```
kesl-control [-R] --add-kataedr-client-certificate <Dateiname und Dateipfad>
```

Argumente und Schlüssel

`<Dateiname und Dateipfad>` – Name und Pfad des Crypto-Containers (Archiv im pfx-Format), der den geheimen Schlüssel enthält.

Befehl kesl-control --remove-kataedr-client-certificate

Mit diesem Befehl können Sie das Client-Zertifikat löschen, das zum Sichern der Verbindung zum KATA-Server verwendet wird.

Befehlssyntax

```
kesl-control [-R] --remove-kataedr-client-certificate
```

Befehl kesl-control --query-kataedr-client-certificate

Mit diesem Befehl können Sie Informationen zum Client-Zertifikat ausgeben.

Befehlssyntax

```
kesl-control [-R] --query-kataedr-client-certificate
```

Befehl kesl-control --isolation-stat

Mit diesem Befehl können Sie den aktuellen Status der Netzwerkisolation in die Konsole ausgeben: aktiviert oder deaktiviert.

Befehlssyntax

```
kesl-control [-R] --isolation-stat
```

Befehl kesl-control --isolation-off

Mit diesem Befehl können Sie die Netzwerkisolation des Geräts temporär deaktivieren.

Befehlssyntax

```
kesl-control [-R] --isolation-off
```

Befehle der App im Light Agent-Modus zum Schutz virtueller Umgebungen

-V – Präfix, das angibt, dass der Befehl zur Gruppe der Befehle für die App Kaspersky Endpoint Security gehört, die im Light Agent-Modus zum Schutz virtueller Umgebungen ausgeführt wird (im Rahmen von Kaspersky Security for Virtualization Light Agent).

> Diese Befehle können nur ausgeführt werden, wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird.

Befehl kesl-control --ksvla-info

Mit diesem Befehl können Sie Informationen zur Nutzung der App im Light Agent-Modus zum Schutz virtueller Umgebungen ausgeben.

Befehlssyntax

```
kesl-control --ksvla-info
```

Befehl kesl-control --viis-info

Mit diesem Befehl können Sie Informationen über die Verbindung des Light Agents (d. h. von Kaspersky Endpoint Security, das als Light Agent im Rahmen von Kaspersky Security for Virtualization Light Agent verwendet wird) zum Integrationsserver ausgeben.

Befehlssyntax

```
kesl-control --viis-info
```

Befehl kesl-control --svm-info

Mit diesem Befehl können Sie Informationen über die Verbindung des Light Agents (d. h. von Kaspersky Endpoint Security, das als Light Agent im Rahmen von Kaspersky Security for Virtualization Light Agent verwendet wird) zur SVM ausgeben.

Befehlssyntax

```
kesl-control --svm-info
```

Anhang 3. Konfigurationsdateien und Standardeinstellungen der App

Zur Verwaltung der Ausführung von Kaspersky Endpoint Security werden die folgenden Konfigurationsdateien verwendet:

- Konfigurationsdateien, die die Einstellungen für die Erstkonfiguration der App enthalten:
  - Konfigurationsdatei autoinstall.ini, die bei der Installation der App mithilfe von Kaspersky Security Center verwendet wird.
  - Konfigurationsdatei, die bei der Installation der App über die Befehlszeile verwendet wird.
- Vorinstallierte Konfigurationsdateien, die bei der Erstkonfiguration der App automatisch erstellt werden und die bei der Erstkonfiguration angegebenen Einstellungswerte enthalten. Diese Parameter werden während der Ausführung der Anwendung angewendet.
- Konfigurationsdateien, die Sie mithilfe der Befehle zur Verwaltung von Kaspersky Endpoint Security erstellen können. Diese Konfigurationsdateien können Aufgabeneinstellungen und andere App-Einstellungen enthalten. Sie können diese Dateien ändern und in die App importieren, um die entsprechenden Einstellungen zu ändern.

Regeln zum Ändern von Konfigurationsdateien für die Aufgaben der App

Beachten Sie folgende Regeln zum Bearbeiten von Konfigurationsdateien:

- In der Konfigurationsdatei müssen alle obligatorischen Einstellungen angeben werden. Sie können individuelle Aufgabeneinstellungen ohne Datei mithilfe der Befehlszeile angeben.
- Wenn eine Einstellung zu einem bestimmten Abschnitt gehört, geben Sie ihn nur in jenem Abschnitt an. Innerhalb eines Abschnitts können Sie die Einstellungen in beliebiger Reihenfolge anordnen.
- Schließen Sie Namen der Abschnitte in eckige Klammern [ ] ein.
- Geben Sie die Einstellungswerte im Format `<Name der Einstellung>=<Wert der Einstellung>` an (Leerzeichen im Namen und in den Werten einer Einstellung werden nicht verarbeitet).

  Beispiel:
  ```
  [ScanScope.item_0000]
  AreaDesc=Home
  AreaMask.item_0000=*doc
  Path=/home
  ```

  Leerzeichen und Tabulator werden vor dem ersten Anführungszeichen und nach dem letzten Anführungszeichen des Zeilenwerts sowie am Anfang und Ende des Zeilenwerts, der nicht in Anführungszeichen steht, ignoriert.
- Wenn Sie einem Parameter mehrere Werte zuweisen müssen, wiederholen Sie die Einstellung entsprechend der Anzahl der Werte, die Sie angeben möchten.

  Beispiel:
  ```
  AreaMask.item_0000=*xml
  AreaMask.item_0001=*doc
  ```
- Beachten Sie bei der Angabe von Werten für folgende Einstellungstypen die Groß- und Kleinschreibung:

- Namen (Masken) der zu untersuchenden und der auszuschließenden Objekte
- Namen (Masken) von Bedrohungen

Für die Werten der verbleibenden Einstellungen ist die Groß- und Kleinschreibung unwesentlich.

- Geben Sie die Werte für Boolesche Einstellungen folgendermaßen an: `Yes / No`.
- Verwenden Sie Anführungszeichen, um Werte für Zeichenfolgen mit Leerzeichen einzuschließen, (z.B. Namen von Dateien oder Verzeichnissen und ihre Pfade, Datum und Zeit im Format "JJJJ-MM-TT HH:MM:SS").

  Alle anderen Werte können Sie sowohl mit als auch ohne Anführungszeichen eingeben.

  Beispiel:
  ```
  AreaDesc=" Mail-Datenbanken untersuchen "
  ```

  Ein einzelnes Anführungszeichen am Beginn oder am Ende einer Zeile gilt als Fehler.

Vorinstallierte Konfigurationsdateien

Nach der Ersteinrichtung werden in der App folgende Konfigurationsdateien erstellt:

- /var/opt/kaspersky/kesl/common/agreements.ini

  Die Konfigurationsdatei agreements.ini enthält Einstellungen für den Endbenutzer-Lizenzvertrag, die Datenschutzrichtlinie und die Erklärung zu Kaspersky Security Network.

- /var/opt/kaspersky/kesl/common/kesl.ini

  Die Konfigurationsdatei kesl.ini enthält die in der nachfolgenden Tabelle angeführten Einstellungen.

Bei Bedarf können Sie in diesen Dateien die Werte der Einstellungen ändern.

Es wird empfohlen, die Änderung der Standardwerte unter Anleitung von Spezialisten des Technischen Supports nach den von ihnen erhaltenen Anweisungen vorzunehmen.

Parameter der Konfigurationsdatei Kesl.ini

Einstellung	Beschreibung	
Der Abschnitt **[General]** enthält die folgenden Einstellungen:		
`Locale`	Der Sprachstandard für die Lokalisierung von Texten, die von Kaspersky Endpoint Security an Kaspersky Security Center gesendet werden (Ereignisse, Benachrichtigungen, Ergebnisse der Aufgabenausführung usw.).	Das Gebietsschema wird mi angegeben. Wird die Einstellung `Locale` Gebietsschema des Betrieb App keine Sprachversion de konnte oder das Betriebssy unterstützt, wird standardm

	Die Lokalisierung der grafischen Benutzeroberfläche und der Befehlszeile der App hängt von der Lokalisierung ab, die in der Umgebungsvariablen `LANG` angegeben ist. Wenn in der Umgebungsvariablen `LANG` eine Lokalisierung angegeben ist, die von Kaspersky Endpoint Security nicht unterstützt wird, werden die grafische Benutzeroberfläche und die Befehlszeile in der englischen Lokalisierung angezeigt.	
`PackageType`	Format des installierten App-Pakets. Das Konfigurieren dieser Option hat keinen Einfluss auf die Ausführung der App. Der Wert des Parameters wird während der Erstkonfiguration der App automatisch ausgefüllt.	`rpm` – Paket wurde im RPM- `deb` – Paket wurde im DEB-
`UseFanotify`	Verwendung der fanotify-Technologie. Das Konfigurieren dieser Option hat keinen Einfluss auf die Ausführung der App. Der Wert des Parameters wird während der Erstkonfiguration der App automatisch ausgefüllt.	`true/yes` – Das Betriebssy Technologie. `false/no` – Das Betriebssy Technologie nicht.
`KsvlaMode`	Nutzungsmodus von Kaspersky Endpoint Security. Das Konfigurieren dieser Option hat keinen Einfluss auf die Ausführung der App. Der Wert des Parameters wird während der Erstkonfiguration der App automatisch ausgefüllt.	`true/yes` – App wird im Lig virtueller Umgebungen verw `false/no` – App wird im St
`StartupTraces`	Aktiviert die Erstellung von Protokolldateien beim Start der App.	`true/yes` – Protokolldateie `false/no` (Standardwert) - der App erstellen.
`RevealSensitiveInfoInTraces`	Anzeigen von Informationen in Ablaufverfolgungsdateien, die personenbezogene Daten enthalten können (z. B. Kennwörter).	`true/yes` – Informationen personenbezogene Daten ir App enthalten. `false/no` (Standardwert) - möglicherweise personenbe Ablaufverfolgungsdateien e
`AsyncTraces`	Aktivieren der asynchronen Ablaufverfolgung, bei welcher Informationen asynchron in Ablaufverfolgungsdateien geschrieben werden.	`true/yes` – asynchrone Ab `false/no` (Standardwert) - nicht aktivieren.
`CoreDumps`	Aktiviert die Erstellung einer Dump-Datei im Falle eines App-Absturzes.	`true/yes` – Im Falle eines A erstellen. `false/no` (Standardwert) - keine Dump-Datei erstellen.
`CoreDumpsPath`	Pfad zum Verzeichnis, in dem die Dump-Dateien gespeichert werden.	Standardwert: /var/opt/kas

		Für den Zugriff auf das Star Dump-Dateien sind Root-Re
`MinFreeDiskSpace`	Die minimale Größe an Festplattenspeicher, die nach dem Schreiben der Dump-Datei verbleiben soll, in Megabyte.	Standardwert: 300.
`ScanMemoryLimit`	Maximaler Speicherverbrauch durch die App in Megabyte.	Standardwert: 8192.
`MachineId`	Eindeutige ID des Geräts des Benutzers.	Der Parameterwert wird wäl automatisch ausgefüllt.
`SocketPath`	Der Pfad zum Socket für die Remote-Verbindung, der beispielsweise die GUI und das Tool kesl-control verbindet.	Standardwert: /var/run/bl4
`MaxInotifyWatches`	Begrenzung der Anzahl an Änderungseinträgen für Dateien und Verzeichnisse (user watches), die in der Datei /proc/sys/fs/inotify/max_user_watches angegeben sind.	Standardwert: 300000.
`MaxInotifyInstances`	Begrenzung der Anzahl an Änderungseinträgen für Dateien und Verzeichnisse pro Benutzer.	Standardwert: 2048.
`ExecEnvMax`	Anzahl der Umgebungsvariablen, welche die App von einem Befehlsaufruf erfasst.	Standardwert: 50.
`ExecArgMax`	Anzahl der Argumente, welche die App von einem exec-Aufruf erfasst.	Standardwert: 50.
`DisableFileAvActions`	Deaktivieren der Desinfektions- und Dateilöschfunktionen für Komponenten der App, nachdem sie installiert wurde. Wenn die Desinfektions- und Dateilöschfunktionen deaktiviert sind und eine Bedrohung erkannt wird, versucht die App nicht, Dateien zu desinfizieren oder zu löschen, in denen eine Bedrohung erkannt wurde, sondern informiert den Benutzer lediglich darüber, dass eine Bedrohung erkannt wurde.	`yes` – Funktionen für das D Dateien beim Anwendungss deaktivieren. `no` (Standardwert) – Funkti Löschen von Dateien beim A Installation nicht deaktiviere
`AdditionalDNSLookup`	Verwendung von öffentlichem DNS. Wenn der Zugriff auf Server über das System-DNS fehlschlägt, verwendet die App das öffentliche DNS. Dies ist erforderlich, um die App-Datenbanken zu aktualisieren und das Sicherheitsniveau des Geräts aufrechtzuerhalten. Die App verwendet die folgenden öffentlichen DNS in der Reihenfolge, in der sie umgangen werden: • Google Public DNS™ (8.8.8.8).	`true/yes` – Öffentliches D Server verwenden. `false/no` (Standardwert) - Zugriff auf Kaspersky-Serve

	• Cloudflare® DNS (1.1.1.1). • Alibaba Cloud® DNS (223.6.6.6). • Quad9® DNS (9.9.9.9). • CleanBrowsing (185.228.168.168).	Anfragen der App könner externe IP-Adresse des B eine TCP/UDP-Verbindun herstellt. Diese Daten sinc die Zertifikate von Webre zu überprüfen. Wenn die A Server verwendet, werde durch die Datenschutzric Wenn verhindert werden öffentlichen DNS-Server Technischen Support eine
Der Abschnitt **[Network]** enthält die folgenden Einstellungen:		
`WtpFwMark`	Markierung in den Regeln des Tools "iptables", um den Datenverkehr an die App umzuleiten und durch die Komponente Schutz vor Web-Bedrohungen zu verarbeiten. Sie müssen diese Markierung möglicherweise ändern, wenn auf demselben Gerät zusammen mit den installierten Apps eine andere Software ausgeführt wird, die das neunte Bit der TCP-Paketmaske verwendet, und ein Konflikt auftritt.	Der Wert wird als Dezimal- o vorangestelltem 0x angegeb Der Standardwert ist 0x100
`NtpFwMark`	Markierung in den Regeln des Tools "iptables", um den Datenverkehr an die App umzuleiten und durch die Komponente Schutz vor Netzwerkbedrohungen zu verarbeiten. Sie müssen diese Markierung möglicherweise ändern, wenn auf demselben Gerät zusammen mit den installierten Apps eine andere Software ausgeführt wird, die das neunte Bit der TCP-Paketmaske verwendet, und ein Konflikt auftritt.	Der Wert wird als Dezimal- o vorangestelltem 0x angegeb Der Standardwert ist 0x200
`BypassFwMark`	Pakete, die von der App erstellt oder bereits untersucht wurden, markieren, um sie von einer erneuten Untersuchung durch die App auszuschließen.	Der Wert wird als Dezimal- o vorangestelltem 0x angegeb Der Standardwert ist 0x400
`BypassNFlogMark`	Markierung für Pakete, die von der App erstellt oder bereits untersucht wurden, um ihre Einträge aus dem Journal des Tools iptable auszuschließen.	Der Wert wird als Dezimal- o vorangestelltem 0x angegeb Der Standardwert ist 0x800
`ProxyRouteTable`	Routing-Tabellennummer.	Standardwert: 101.
Der Abschnitt **[Virtualization]** enthält die folgenden Einstellungen:		
`ServerMode`	Rolle einer geschützten virtuellen Maschine, auf der Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen	`true/yes` – Die virtuelle Ma `false/no` – Die virtuelle Ma verwendet.

	verwendet wird: Server oder Workstation. Das Konfigurieren dieser Option hat keinen Einfluss auf die Ausführung der App. Der Wert des Parameters wird während der Erstkonfiguration der App automatisch ausgefüllt.	
`VdiMode`	Aktivieren des Modus zum Schutz von VDI-Infrastrukturen bei Verwendung der App im Light Agent-Modus zum Schutz virtueller Umgebungen. Das Konfigurieren dieser Option hat keinen Einfluss auf die Ausführung der App. Der Wert des Parameters wird während der Erstkonfiguration der App automatisch ausgefüllt.	`true/yes` – Modus zum Sc aktiviert. `false/no` – Modus zum Sc deaktiviert.
Der Abschnitt **[Watchdog]** enthält die folgenden Einstellungen:		
`TimeoutAfterHeadshot`	Die maximale Wartezeit für die Beendigung des Prozesses "kesl" ab dem Zeitpunkt, an dem der Watchdog-Server das HEADSHOT-Signal an den Prozess "kesl" sendet.	Standardwert: 2 Min.
`StartupTimeout`	Maximale Wartezeit auf den Start der App (in Minuten), nach deren Überschreitung der Prozess "kesl" neu gestartet wird.	Standardwert: 3 Min.
`TimeoutAfterKill`	Maximale Wartezeit für die Beendigung des verwalteten Prozesses "kesl" ab dem Zeitpunkt, an dem der Watchdog-Server das SIGKILL-Signal an den Prozess "kesl" sendet. Wenn der Prozess "kesl" nach dieser Zeit nicht beendet wurde, wird die durch den Parameter --failed-kill angegebene Aktion ausgeführt.	Standardwert: 2 Tage.
`PingInterval`	Intervall, in dem die App versucht, als Antwort auf eine empfangene PING-Nachricht eine PONG-Nachricht an den Server zuzustellen.	Standardwert: 2000 ms.
`MaxRestartCount`	Maximale Anzahl erfolgloser aufeinanderfolgender Versuche, die App zu starten.	Standardwert: 5.
`ActivityTimeout`	Maximales Zeitintervall, während dem die App eine Nachricht an den Watchdog-Server senden muss. Erfolgt in diesem Zeitintervall keine Meldung der Anwendung, startet der Watchdog-Server die Prozedur zur Beendigung des Prozesses "kesl".	Standardwert: 2 Min.
`ConnectTimeout`	Maximales Zeitintervall ab dem Start des Prozesses "kesl" bis zu dem Moment, in	Standardwert: 3 Min.

	dem die Anwendung eine Verbindung mit dem Watchdog-Server herstellt. Wenn es der Anwendung innerhalb dieses Zeitintervalls nicht gelingt, eine Verbindung herzustellen, startet der Watchdog-Server den Vorgang zum Beenden des Prozesses "kesl".	
`RegisterTimeout`	Das maximale Zeitintervall ab dem Zeitpunkt, an dem die App eine Verbindung zum Watchdog-Server herstellt, bis der Server die REGISTER-Nachricht empfängt.	Standardwert: 500 ms.
`TimeoutAfterShutdown`	Die maximale Wartezeit für die Beendigung des Prozesses "kesl" ab dem Zeitpunkt, an dem der Watchdog-Server das SHUTDOWN-Signal an den Prozess "kesl" sendet.	Standardwert: 2 Min.
`MaxMemory`	Beschränkung der Verwendung des residenten Speichers des Prozesses "kesl". Wenn der residente Speicher des verwalteten Prozesses dieses Limit überschreitet, startet der Watchdog-Server den Vorgang zum Beenden des Prozesses "kesl".	`off` – Die Nutzung des resi beschränkt. `< Wert >%` – Die verfügbare 100 Prozent der Speichergr `< Wert >MB` – Wert in Mega `lowest/< Wert >%/< Wert` zwischen dem Prozentwert `highest/< Wert >%/< Wer` dem Prozentwert und dem I `auto` – bis zu 50% des verf 2 GB und maximal 16 GB. Der Standardwert ist `auto`.
`MaxVirtualMemory`	Beschränkung für die Verwendung des virtuellen Speichers des Prozesses "kesl". Wenn der virtuelle Speicher des verwalteten Prozesses dieses Limit überschreitet, startet der Watchdog-Server den Vorgang zum Beenden des Prozesses "kesl".	`off` (Standardwert) – Die N unbegrenzt. `< Wert >MB` – Wert in Mega
`MaxSwapMemory`	Größenbeschränkung für die Auslagerungsdatei des verwalteten Prozesses "kesl". Wenn die Auslagerungsdatei des verwalteten Prozesses dieses Limit überschreitet, startet der Watchdog-Server den Vorgang zum Beenden des Prozesses "kesl".	`off` (Standardwert) – Die G nicht begrenzt. `< Wert >%` – Die verfügbare Prozent der Speichergröße. `< Wert >MB` – Wert in Mega `lowest/< Wert >%/< Wert` zwischen dem Prozentwert `highest/< Wert >%/< Wer` dem Prozentwert und dem I
`TrackProductCrashes`	Überwachung der Anwendungsstabilität aktivieren.	`true/yes` – Überwachung aktivieren. `false/no` (Standardwert) - Anwendungsstabilität deakt

	Wenn die Überwachung der Anwendungsstabilität aktiviert ist, überwacht der Watchdog-Server die Anzahl der ungeplanten Unterbrechungen der App.	
`ProductHealthLogFile`	Pfad zu der Datei, die zur Überwachung der Anwendungsstabilität verwendet wird.	Standardwert: /var/opt/kas
`WarnThreshold`	Zeitintervall (in Sekunden), in dem die App die Anzahl der ungeplanten Unterbrechungen zählen soll, bevor eine Warnung über Instabilität angezeigt wird.	Standardwert: 3.600 Sekun
`WarnAfter_#_crash`	Anzahl der ungeplanten Unterbrechungen der App, die erforderlich sind, um eine Benachrichtigung über eine instabile Ausführung der App anzuzeigen.	Standardwert: 10. Wenn der Wert auf 0 geset Benachrichtigung über die I
`WarnRemovingThreshold`	Zeitintervall (in Sekunden), nach dem der Status "Instabil" der App entfernt wird.	Standardwert: 86400 Seku
Der Abschnitt **[Environment]** ist in der Konfigurationsdatei standardmäßig nicht vorhanden.		
`ExperimentalContainerdSupport`	Aktivieren der Unterstützung für die containerd-Umgebung beim Ausführen der Komponente Container-Überwachung. Diese Einstellung ist standardmäßig nicht in der Konfigurationsdatei vorhanden. Wenn Sie beim Ausführen der Komponente "Container-Überwachung" die Umgebung "containerd" verwenden möchten, müssen Sie in der Konfigurationsdatei den Abschnitt `[Environment]` manuell hinzufügen und ihn um den Parameter `ExperimentalContainerdSupport` ergänzen.	`true/yes` – Unterstützung Komponente "Container-Üb `false/no` – Unterstützung Komponente "Container-Üb

Standardeinstellungen der Befehlszeilenaufgaben

Dieser Abschnitt enthält die Standardeinstellungen aller vordefinierten Aufgaben, die für die Verwaltung von Kaspersky Endpoint Security über die Befehlszeile vorgesehen sind.

Die Aufgaben *Rollback* und *License* haben keine Einstellungen.

Standardeinstellungen der Aufgabe File_Threat_Protection (ID:1)

```
ScanArchived=No
```

```
ScanSfxArchived=No

ScanMailBases=No

ScanPlainMail=No

SkipPlainTextFiles=No

TimeLimit=60

SizeLimit=0

FirstAction=Recommended

SecondAction=Block

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanByAccessType=SmartCheck

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Standardeinstellungen der Aufgabe Scan_My_Computer (ID:2)

```
ScanFiles=Yes

ScanBootSectors=Yes

ScanComputerMemory=Yes

ScanStartupObjects=Yes
```

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Standardeinstellungen der Aufgabe Scan_File (ID:3)

```
ScanFiles=Yes

ScanBootSectors=No
```

```
ScanComputerMemory=No

ScanStartupObjects=No

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Standardeinstellungen der Aufgabe Critical_Areas_Scan (ID:4)

```
ScanFiles=No
ScanBootSectors=Yes
ScanComputerMemory=Yes
ScanStartupObjects=Yes
ScanArchived=Yes
ScanSfxArchived=Yes
ScanMailBases=No
ScanPlainMail=No
TimeLimit=0
SizeLimit=0
FirstAction=Recommended
SecondAction=Skip
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
UseGlobalExclusions=Yes
UseOASExclusions=Yes
DeviceNameMasks.item_0000=/**
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
```

Standardeinstellungen der Aufgabe Update (ID:6)

```
SourceType="KLServers"

UseKLServersWhenUnavailable=Yes

ApplicationUpdateMode=DownloadOnly

ConnectionTimeout=10
```

Standardeinstellungen der Aufgabe Backup (ID:10)

```
DaysToLive=90

BackupSizeLimit=0

BackupFolder=/var/opt/kaspersky/kesl/common/objects-backup/
```

Standardeinstellungen der Aufgabe System_Integrity_Monitoring (ID:11)

```
UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=Kaspersky internal objects

UseScanArea=Yes

Path=/opt/kaspersky/kesl/

AreaMask.item_0000=*
```

Standardeinstellungen der Aufgabe Firewall_Management (ID:12)

```
DefaultIncomingAction=Allow

DefaultIncomingPacketAction=Allow

OpenNagentPorts=Yes

[NetworkZonesTrusted]

[NetworkZonesLocal]

[NetworkZonesPublic]
```

Standardeinstellungen der Aufgabe Anti_Cryptor (ID:13)

```
ActionOnDetect=Block

BlockTime=30

UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=All shared directories

UseScanArea=Yes

Path=AllShared

AreaMask.item_0000=*
```

Standardeinstellungen der Aufgabe Web_Threat_Protection (ID:14)

```
UseTrustedAddresses=Yes

ActionOnDetect=Block

CheckMalicious=Yes

CheckPhishing=Yes

UseHeuristicForPhishing=Yes

CheckAdware=No

CheckOther=No
```

Standardeinstellungen der Aufgabe Device_Control (ID:15)

```
OperationMode=Block

[DeviceClass]

HardDrive=DependsOnBus

RemovableDrive=DependsOnBus

Printer=DependsOnBus

FloppyDrive=DependsOnBus

OpticalDrive=DependsOnBus
```

```
Modem=DependsOnBus

TapeDrive=DependsOnBus

MultifuncDevice=DependsOnBus

SmartCardReader=DependsOnBus

PortableDevice=DependsOnBus

WiFiAdapter=DependsOnBus

NetworkAdapter=DependsOnBus

BluetoothDevice=DependsOnBus

ImagingDevice=DependsOnBus

SerialPortDevice=DependsOnBus

ParallelPortDevice=DependsOnBus

InputDevice=DependsOnBus

SoundAdapter=DependsOnBus

[DeviceBus]

USB=Allow

FireWire=Allow

[Schedules.item_0000]

ScheduleName=Default

DaysHours=All

[HardDrivePrincipals.item_0000]

Principal=\Everyone

[HardDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[RemovableDrivePrincipals.item_0000]

Principal=\Everyone

[RemovableDrivePrincipals.item_0000.AccessRules.item_0000]
```

```
UseRule=Yes

ScheduleName=Default

Access=Allow

[FloppyDrivePrincipals.item_0000]

Principal=\Everyone

[FloppyDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[OpticalDrivePrincipals.item_0000]

Principal=\Everyone

[OpticalDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow
```

Standardeinstellungen der Aufgabe Removable_Drives_Scan (ID:16)

```
ScanRemovableDrives=NoScan

ScanOpticalDrives=NoScan

BlockDuringScan=No
```

Standardeinstellungen der Aufgabe Network_Threat_Protection (ID:17)

```
ActionOnDetect=Block

BlockAttackingHosts=Yes

BlockDurationMinutes=60

UseExcludeIPs=No
```

Standardeinstellungen der Aufgaben Container_Scan (ID:18) und Custom_Container_Scan (ID:19)

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanContainers=Yes

ContainerNameMask=*

ScanImages=Yes

ImageNameMask=*

DeepScan=No

ContainerScanAction=StopContainerIfFailed

ImageAction=Skip

UseGlobalExclusions=Yes
```

Sie können die Einstellungen dieser Konfigurationsdatei auch für die Aufgabe zur benutzerdefinierten Untersuchung von Containern verwenden.

Standardeinstellungen der Aufgabe Behavior_Detection (ID:20)

```
UseTrustedPrograms=No

TaskMode=Block
```

Standardeinstellungen der Aufgabe Application_Control (ID:21)

```
AppControlMode=DenyList

AppControlRulesAction=ApplyRules
```

Standardeinstellungen der Aufgabe Inventory_Scan (ID:22)

```
ScanScripts=Yes

ScanBinaries=Yes

ScanAllExecutable=Yes

CreateGoldenImage=No

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/usr/bin

AreaMask.item_0000=*
```

Standardeinstellungen der Aufgabe KATAEDR (ID:24)

```
UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

EnableTelemetry=Yes

[Endpoints.item_0000]

Address=
```

```
Port=443

[EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15
```

Standardeinstellungen der Aufgabe Web_Control (ID:26)

```
WebControlDefaultAction=Allow

ComplaintRecipient=
```

Allgemeine App-Einstellungen

Die allgemeinen App-Einstellungen bestimmen die Ausführung der App als Ganzes und die Ausführung einzelner Funktionen.

Allgemeine App-Einstellungen

Einstellung	Beschreibung	
`SambaConfigPath`	Verzeichnis, in dem die Samba-Konfigurationsdatei gespeichert ist. Die Samba-Konfigurationsdatei ist erforderlich, um zu gewährleisten, dass die Werte `AllShared` bzw. `Shared:SMB` für den Parameter `Path` übernommen werden.	Standardmäßig ist das das Sta Konfigurationsdatei angegeben Standardwert: /etc/samba/sm Nach der Änderung dieser Eins erforderlich.
`NfsExportPath`	Verzeichnis, in dem die NFS-Konfigurationsdatei gespeichert ist. Die NFS-Konfigurationsdatei ist erforderlich, um zu gewährleisten, dass die Werte `AllShared` bzw. `Shared:NFS` für den Parameter `Path` übernommen werden.	Standardmäßig ist das das Sta Konfigurationsdatei angegeben Standardwert: /etc/exports Nach der Änderung dieser Eins erforderlich.
`TraceLevel`	Aktiviert die App-Protokollierung und den Detaillierungsgrad der Protokolldateien.	`Detailed` – Erstellt eine detai `MediumDetailed` – Erstellt ei und Fehlermeldungen. `NotDetailed` – Erstellt eine P enthält. `None` (Standardwert) – Keine F
`TraceFolder`	Verzeichnis, in dem die Protokolldateien der App	Standardwert: /var/log/kasper

	gespeichert sind.	Wenn Sie ein anderes Verzeich das Benutzerkonto, unter dem ausgeführt wird, eine Lese- un Verzeichnis besitzt. Für den Zu zum Speichern von Ablaufverf erforderlich. Nach der Änderung dieser Eins erforderlich.
`TraceMaxFileCount`	Gibt die Maximalanzahl der Protokolldateien der App an.	1–10.000 Standardwert: 10. Nach der Änderung dieser Eins erforderlich.
`TraceMaxFileSize`	Legt die maximale Größe der Protokolldatei der App fest (in Megabyte).	1–1.000 Standardwert: 500. Nach der Änderung dieser Eins erforderlich.
`BlockFilesGreaterMaxFileNamePath`	Sperrt den Zugriff auf Dateien, deren vollständige Pfadlänge den in Bytes angegebenen Wert der Einstellung übersteigt. Wenn der vollständige Pfad der Datei, die untersucht werden soll, den Wert dieser Einstellung übersteigt, wird die Datei von der Untersuchungsaufgabe bei der Untersuchung übersprungen. Diese Einstellung ist nicht für Betriebssysteme verfügbar, welche die fanotify-Technologie nutzen.	4096–33554432 Standardwert: 16384. Nachdem Sie den Wert für die muss die Aufgabe "Schutz vor gestartet werden.
`DetectOtherObjects`	Aktiviert die Erkennung legitimer Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können.	`Yes` – Aktiviert die Erkennung Angreifern für Kompromittieru ausgenutzt werden können. `No` (Standardwert) – Aktiviert Anwendungen, die von Angreif Geräten oder Daten ausgenutz
`NamespaceMonitoring`	Aktiviert die Untersuchung von Namespaces und Containern. Die App prüft keine Namespaces und Container, es sei denn, auf dem Betriebssystem sind Komponenten für die Arbeit mit Containern und Namespaces installiert.	`Yes` (Standardwert) – Untersu Containern aktivieren. `No` – Untersuchung von Names deaktivieren.
`FileBlockDuringScan`	Aktivieren des Modus des Moduls zum Abfangen von Dateioperationen mit Blockieren	`Yes` (Standardwert) – Zugriff a Untersuchung blockieren.

	des Zugriffs auf Dateien während der Untersuchung. Der Modus des Moduls zum Abfangen von Dateioperationen hat Auswirkungen auf die Ausführung der Komponenten Schutz vor bedrohlichen Dateien und Gerätekontrolle.	`No` – Zugriff auf Dateien währe blockieren. Der Zugriff auf eine Überprüfung erfolgt im asynch Moduls zum Abfangen von Dat Ausführung weniger Auswirkun besteht jedoch das Risiko, dass desinfiziert oder entfernt wird, während der Untersuchung ihre eine Entscheidung über den St
`UseKSN`	Verwendung von Kaspersky Security Network aktivieren.	`Basic` – Verwendung von Kasp Standard-Modus aktivieren. `Extended` – Verwendung von erweiterten Modus aktivieren. `No` (Standardwert) – Verwendu Network deaktivieren.
`CloudMode`	Aktivieren des Cloud-Modus der App. Der Cloud-Modus ist verfügbar, wenn KSN aktiviert ist. Wenn Sie den Cloud-Modus verwenden möchten, stellen Sie sicher, dass KSN auf Ihrem Gerät verfügbar ist. Die Einstellung wird nur angewendet, wenn die App im Standard-Modus verwendet wird.	`Yes` – Aktivieren des Ausführu Endpoint Security eine schlank Datenbanken verwendet. `No` (Standardwert) – vollständ verwenden. Der Cloud-Modus wird auto deaktiviert ist.
`UseMDR`	Aktivieren der Komponente "Managed Detection and Response" für die Integration mit Kaspersky Managed Detection and Response.	`Yes` – die Komponente "Manag aktivieren. `No` (Standardwert) – die Komp Response" deaktivieren
`UseProxy`	Aktiviert die Verwendung eines Proxy-Servers durch Komponenten von Kaspersky Endpoint Security. Ein Proxy-Server kann verwendet werden, um mit Kaspersky Security Network und Kaspersky Endpoint Detection and Response (KATA) zu interagieren, sowie um die App zu aktivieren und die Datenbanken und Module der App zu aktualisieren.	`Yes` – Nutzung eines Proxy-Se `No` (Standardwert) – Verwendu Wenn `Yes` ausgewählt ist, erfo Endpoint Detection and Respo Server.

	Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, wird die Verwendung eines Proxy-Servers für die Verbindung mit Kaspersky Security Network, zur SVM und zum Integrationsserver nicht unterstützt.	
`ProxyServer`	Proxy-Server-Einstellungen im Format `[<Benutzer>[:<Kennwort>]@]<Proxy-Server-Adresse>[:<Port>]`. Für die Verbindung über einen HTTP-Proxy wird empfohlen, ein separates Konto zu verwenden, das nicht zur Authentifizierung in anderen Systemen verwendet wird. Der HTTP-Proxy verwendet eine unsichere Verbindung und dessen Konto kann kompromittiert werden.	—
`MaxEventsNumber`	Maximale Anzahl von Ereignissen, die von der App gespeichert werden. Wenn die angegebene Anzahl von Ereignissen übertroffen wird, löscht die App die ältesten Ereignisse.	Standardwert: 500000. Bei Angabe des Wertes 0 werd
`LimitNumberOfScanFileTasks`	Maximale Anzahl der Aufgaben zur benutzerdefinierten Untersuchung, die ein nicht privilegierter Benutzer gleichzeitig auf dem Gerät starten kann. Durch diese Einstellung wird die Anzahl der Aufgaben, die ein Benutzer mit Root-Rechten starten kann, nicht beschränkt.	0–4294967295 Standardwert: 0. Wenn der Wert 0 angegeben is Benutzer keine Aufgaben zur b starten. Wenn Sie während der App-Ins haben, wird für den Parameter der Standardwert `5` verwende
`UseSyslog`	Aktivierung der Protokollierung von Informationen über Ereignisse in syslog. Für den Zugriff auf syslog sind Root-Rechte erforderlich.	`Yes` – Protokollieren von Inforr aktivieren. `No` (Standardwert) – Protokolli Ereignisse im syslog deaktiviere
`EventsStoragePath`	Verzeichnis mit der Datenbank,	Standardwert: /var/opt/kaspe

	in der die App die Informationen über Ereignisse speichert. Für den Zugriff auf die Standarddatenbank mit Ereignissen sind Root-Rechte erforderlich.	
`ExcludedMountPoint.item_#`	Der Mountpunkt, den Sie vom Untersuchungsbereich ausschließen möchten. Die Ausnahme wird bei der Ausführung folgender Komponenten und Aufgaben angewendet: bei den Komponenten Schutz vor bedrohlichen Dateien, Schutz vor Verschlüsselung und Container-Überwachung sowie für die Aufgabe Untersuchung von Wechseldatenträgern. Weiterhin wird die Ausnahme während der Ausführungen der Untersuchungsaufgaben (Aufgaben vom Typ ODS oder ContainerScan) konfiguriert. Sie können mehrere Mountpunkte angeben, die von der Untersuchung ausgeschlossen werden sollen. Die Mountpunkte müssen genau so angegeben werden, wie sie in der Ausgabe des Befehls `mount` angezeigt werden. Die Einstellung `ExcludedMountPoint.item_#` ist standardmäßig nicht angegeben.	`AllRemoteMounted` – Alle Re Gerät über SMB- oder NFS-Pr vom Interceptor für Dateiopera `Mounted:NFS` – Alle Remote- über NFS-Protokolle gemounte Abfangen von Dateioperatione `Mounted:SMB` – Alle Remote- über SMB-Protokolle gemount Abfangen von Dateioperatione `Mounted:<Typ des Dateis` Verzeichnisse mit dem angege Modul zum Abfangen von Date `/mnt` – Objekte im Mountpunk Unterverzeichnissen), welcher Wechseldatenträger dient, wer ausgeschlossen. `<Pfad mit der Maske /mnt /mnt/**/user_share>` – Obj der angegebenen Maske entsp ausgeschlossen.

		Verwenden Sie das Zeichen Datei- oder Verzeichnisname Sie können einen Stern `*` ve Anzahl an Zeichen (inklusive Zeichen `/` im Datei- oder Ve Beispiel: `/dir/*/file` oder Sie können zwei aufeinander um eine beliebige Anzahl an Menge) im Datei- oder Verze Zeichens `/` zu ersetzen. Beis `/dir/file**/`. Die Maske `**` kann nur ein ei verwendet werden. Beispiel: nicht korrekt. Um den Mountpunkt `/dir` a `/dir` (ohne die Sternchen) a Die Maske `/dir/*` schließt a tiefer als `/dir` aus, aber nich Die Maske `/dir/**` schließt Verschachtelungsebenen un Mountpunkt `/dir` selbst. Sie können das Symbol `?` an einem Datei- oder Verzeichn
`MemScanExcludedProgramPath.item_#`	Prozess-Speicher von der Untersuchung ausschließen. Der Arbeitsspeicher des angegebenen Prozesses wird von der App nicht untersucht.	`<vollständiger Pfad des` angegebenen Verzeichnis von der Angabe des Pfades könner Verwenden Sie das Zeichen Datei- oder Verzeichnisname Sie können einen Stern `*` ve Anzahl an Zeichen (inklusive Zeichen `/` im Datei- oder Ve Beispiel: `/dir/*/file` oder Sie können zwei aufeinander um eine beliebige Anzahl an Menge) im Datei- oder Verze Zeichens `/` zu ersetzen. Beis `/dir/file**/`. Die Maske `**` kann nur ein ei verwendet werden. Beispiel: nicht korrekt. Sie können das Symbol `?` an einem Datei- oder Verzeichn

`UseOnDemandCPULimit`	Aktiviert die Begrenzung der Nutzung von CPU-Ressourcen für die Aufgabentypen *ODS*, *ContainerScan* und *InventoryScan*.	`Yes` – Aktiviert die Begrenzung für die Aufgabentypen *ODS*, *C* `No` (Standardwert) – Deaktivie CPU-Ressourcen für Aufgaben
`OnDemandCPULimit`	Maximale Auslastung aller Prozessorkerne (in Prozent) bei der Ausführung der Aufgabentypen *ODS*, *ContainerScan* und *InventoryScan*.	10 – 100 Standardwert: 100.
`UseEdrOptimum`	Aktivieren der Komponente "EDR Optimum" für die Integration mit Kaspersky Endpoint Detection and Response Optimum.	`Ja` – Komponente "EDR Optim `No` (Standardwert) – Kompone

Allgemeine Einstellungen der Container-Untersuchung

Für die Untersuchung von Namespaces und Containern in Echtzeit werden die allgemeinen Einstellungen für die Untersuchung von Containern verwendet.

Allgemeine Einstellungen für die Untersuchung von Containern und Namespaces

Einstellung	Beschreibung	Werte
`OnAccessContainerScanAction`	Aktion, die für einen Container ausgeführt werden soll, wenn ein infiziertes Objekt erkannt wird. Dieser Parameter ist verfügbar, wenn die App im Rahmen einer Lizenz verwendet wird, die diese Funktion einschließt. Bei der Untersuchung von Objekten in Containern werden die Einstellungen der Aufgabe Schutz vor bedrohlichen Dateien verwendet. Die Aktion für einen Container beim Fund eines infizierten Objekts hängt auch von den angegebenen Einstellungen für die Aufgabe zum Schutz vor bedrohlichen Dateien ab (siehe Tabelle unten).	`StopContainerIfFailed` (Standardwert) – der Container wird angehalten, wenn die Desinfektion oder das Löschen eines infizierten Objekts fehlgeschlagen ist. `StopContainer` – der Container wird angehalten, wenn ein infiziertes Objekt erkannt wird. `Skip` – für den Container wird beim Fund eines infizierten Objekts keine Aktion ausgeführt.
`UseDocker`	Verwendung der Docker-Umgebung.	`Yes` (Standardwert) – Docker-Umgebung verwenden `No` – Docker-Umgebung nicht verwenden
`DockerSocket`	Pfad oder URI (Uniform Resource Identifier) des Docker-Sockets.	Der Standardwert ist /var/run/docker.sock.

`UseCrio`	Verwendung der CRI-O-Umgebung.	`Yes` (Standardwert) – CRI-O-Umgebung verwenden `No` – CRI-O-Umgebung nicht verwenden
`CrioConfigFilePath`	Der Pfad zur CRI-O-Konfigurationsdatei.	Standardwert: /etc/crio/crio.conf.
`UsePodman`	Verwendung des Podman-Tools.	`Yes` (Standardwert) – Podman-Tool verwenden `No` – Podman-Tool nicht verwenden
`PodmanBinaryPath`	Pfad zur ausführbaren Datei des Podman-Tools.	Der Standardwert ist /usr/bin/podman.
`PodmanRootFolder`	Pfad zum Stammverzeichnis des Container-Speichers.	Der Standardwert ist /var/lib/containers/storage.
`UseRunc`	Verwendung des runc-Tools.	`Yes` (Standardwert) – runc-Tool verwenden `No` – runc-Tool nicht verwenden
`RuncBinaryPath`	Pfad zur ausführbaren Datei des runc-Tools.	Der Standardwert ist: /usr/bin/runc.
`RuncRootFolder`	Pfad zum Stammverzeichnis des Speichers für den Container-Status.	Der Standardwert ist /run/runc.

Die Aktion, die für einen Container ausgeführt wird, wenn ein infiziertes Objekt erkannt wird, kann sich abhängig von den angegebenen Werten der Parameter `FirstAction` und `SecondAction` der Aufgabe zum Schutz vor bedrohlichen Dateien ändern.

Abhängigkeit der Aktion für Container von der angegebenen Aktion für infizierte Objekte bei Erkennung einer Bedrohung

Wert der Einstellung "FirstAction/SecondAction"	Aktion, die für den Container ausgeführt wird, wenn die Aktion StopContainerIfFailed ausgewählt ist
`Disinfect`	Der Container wird angehalten, wenn die Desinfektion eines infizierten Objekts fehlgeschlagen ist.
`Remove`	Der Container wird angehalten, wenn das Löschen eines infizierten Objekts fehlgeschlagen ist.

Einstellungen der Untersuchung geschützter Verbindungen

Einstellungen der Untersuchung geschützter Verbindungen

Einstellung	Beschreibung	Werte
`EncryptedConnectionsScan`	Aktiviert und deaktiviert die Untersuchung von verschlüsseltem Datenverkehr.	`Yes` (Standardwert) – Untersuchung geschützter Verbindungen aktivieren `No` – Untersuchung geschützter Verbindungen deaktivieren Die App entschlüsselt den verschlüsselten Datenverkehr nicht.

	Für das FTP-Protokoll ist die Untersuchung geschützter Verbindungen standardmäßig deaktiviert.	
`EncryptedConnectionsScanErrorAction`	Aktion, die die App ausführen soll, wenn auf einer Website ein Fehler bei der Untersuchung der geschützten Verbindung auftritt.	`AddToAutoExclusions` (Standardwert) – Die Domain, die den Fehler verursacht hat, wird zur Liste der Domains mit Untersuchungsfehlern hinzugefügt. Die App überwacht den verschlüsselten Netzwerkverkehr nicht, wenn diese Domain besucht wird. `Disconnect` – Netzwerkverbindung blockieren
`CertificateVerificationPolicy`	Gibt an, auf welche Art Kaspersky Endpoint Security die Zertifikate überprüft. Wenn ein Zertifikat selbstsigniert ist, führt die App keine zusätzliche Untersuchung durch.	`FullCheck` (Standardwert) – Die App nutzt das Internet, um die fehlenden Ketten, die zur Überprüfung des Zertifikats erforderlich sind, zu prüfen und herunterzuladen. `LocalCheck` – Die App nutzt zur Überprüfung des Zertifikats nicht das Internet.
`UntrustedCertificateAction`	Aktion, die die App ausführen soll, wenn sie ein nicht vertrauenswürdiges Zertifikat erkennt.	`Allow` (Standardwert) – Netzwerkverbindung zulassen, die beim Aufruf einer Domain mit einem nicht vertrauenswürdigen Zertifikat hergestellt wurde `Block` – Netzwerkverbindung blockieren, die beim Aufruf einer Domain mit einem nicht vertrauenswürdigen Zertifikat hergestellt wurde
`ManageExclusions`	Verwendung von Ausschlüssen bei der Untersuchung von verschlüsseltem Datenverkehr.	`Yes` – Websites, die im Abschnitt `[Exclusions.item_#]` angegeben sind (s. unten), nicht untersuchen `No` (Standardwert) – Alle Websites untersuchen
`MonitorNetworkPorts`	Legt fest, auf welche Weise Kaspersky Endpoint Security Netzwerkports überwacht.	`Selected` (Standardwert) – Nur Netzwerkports überwachen, die im Abschnitt `[NetworkPorts.item_#]` angegeben sind (siehe unten) `All` – Alle Netzwerkports überwachen

		Die Angabe dieses Wertes kann die Auslastung des Betriebssystems erheblich erhöhen.
Der Abschnitt **[Exclusions.item_#]** enthält Domains, die von der Untersuchung ausgeschlossen werden sollen. Die App untersucht keine geschützten Verbindungen, die beim Aufruf bestimmter Domänen hergestellt wurden.		
`DomainName`	Gibt den Domain-Namen an. Bei der Angabe der Domain können Masken verwendet werden.	Der Standardwert ist nicht angegeben.
Der Abschnitt **[NetworkPorts.item_#]** enthält die Netzwerkports, welche die App überwachen soll.		
`PortName`	Beschreibung des Netzwerkports.	Der Standardwert ist nicht angegeben.
`Port`	Nummern der Netzwerkports, welche die App überwachen soll.	`1 – 65535` Der Standardwert ist nicht angegeben.

Einstellungen des Aufgabenzeitplans

Einstellungen des Zeitplans für den Aufgabenstart

Einstellung	Beschreibung	Werte
`RuleType`	Zeitplan für den Aufgabenstart.	`Once` – Führt die Aufgabe einmal aus. `Monthly` – Führt die Aufgabe jeden Monat am angegebenen Tag und zur angegebenen Uhrzeit aus. `Weekly` – Führt die Aufgabe jede Woche am angegebenen Tag und zur angegebenen Uhrzeit aus. `Daily` – Führt die Aufgabe regelmäßig in einem angegebenen Intervall in Tagen aus. `Hourly` – Führt die Aufgabe regelmäßig in einem angegebenen Intervall in Stunden aus, beginnend mit dem angegebenen Datum und der angegebenen Uhrzeit. `Minutely` – Führt die Aufgabe regelmäßig in einem angegebenen Intervall in Minuten aus, beginnend mit der angegebenen Uhrzeit. `Manual` – Aufgabe manuell starten. `PS` – Aufgabe nach dem Starten der App starten.

		`BR` – Aufgabe nach dem Update der App-Datenbanken starten.
`StartTime`	Datum und Uhrzeit des Aufgabenstarts. Die Einstellung `StartTime` ist erforderlich, wenn die Einstellung `RuleType` einen der folgenden Werte hat: Once, Monthly, Weekly, Daily, Hourly, Minutely.	`[<Jahr>/<Monat>/<Tag des Monats>] [hh]:[mm]:[ss]; [<Tag des Monats>|<Wochentag>]; [<Starthäufigkeit>]`
`RandomInterval`	Zeitintervall (in Minuten) von 0 bis zum angegebenen Wert, welches zur Startzeit der Aufgabe hinzugefügt wird, um den gleichzeitigen Start von Aufgaben zu vermeiden.	
`RunMissedStartRules`	Aktiviert den Start einer übersprungenen Aufgabe nach dem Starten der App.	`Yes` – Aktiviert den Start einer übersprungenen Aufgabe nach dem Starten der App. `No` – Aktiviert nicht den Start einer übersprungenen Aufgabe nach dem Starten der App.

Anhang 4. Rückgabecodes der Befehlszeile

Kaspersky Endpoint Security enthält die folgenden Rückgabecodes der Befehlszeile.

0 – Befehl/Aufgabe erfolgreich ausgeführt

1 – Allgemeiner Fehler in den Argumenten des Befehls

2 – Fehler in den übergebenen App-Einstellungen

64 – Kaspersky Endpoint Security wurde nicht gestartet

66 – App-Datenbanken wurden nicht heruntergeladen (wird nur vom Befehl `kesl-control --app-info`) verwendet

67 – Aktivierung 2.0 wurde aufgrund von Netzwerkproblemen fehlerhaft abgeschlossen

68 – Befehlsausführung unmöglich, da die App gemäß einer Richtlinie ausgeführt wird

69 – Die App befindet sich in der Infrastruktur von Amazon Paid Ami

70 – Versuch, eine bereits laufende Aufgabe zu starten, eine laufende Aufgabe zu löschen, die Einstellungen einer laufenden Aufgabe zu ändern, eine beendete Aufgabe zu beenden, eine angehaltene Aufgabe anzuhalten oder eine laufende Aufgabe fortzusetzen

71 – Erklärung zu Kaspersky Security Network nicht akzeptiert

72 – Fund von Bedrohungen während der Ausführung der Aufgabe "Benutzerdefinierte Untersuchung" oder "Benutzerdefinierte Untersuchung von Containern"

73 – Versuch, die Einstellungen der Aufgabe "App-Kontrolle", welche die Ausführung der App beeinflusst, ohne Bestätigung mit dem Flag `--accept` anzugeben

74 – Neustart von Kaspersky Endpoint Security nach einem Update erforderlich

75 – Neustart des Geräts erforderlich

76 - Verbindung verweigert, da nur Benutzer mit Root-Berechtigungen Schreibzugriff auf den angegebenen Pfad haben sollten

77 - Der angegebene Lizenzschlüssel wird bereits auf dem Gerät verwendet

128 – Unbekannter Fehler

65 – Alle übrigen Fehler

Anhang 5. Einstellungen für die Zusammenarbeit mit Kaspersky Anti-Virus für Linux Mail Server

So passen Sie die gemeinsame Ausführung von Kaspersky Endpoint Security und Kaspersky Anti-Virus für Linux Mail Server an:

1. Speichern Sie die Einstellungen der Aufgabe zum Schutz vor bedrohlichen Dateien in der Konfigurationsdatei mithilfe des folgenden Befehls:

   ```
   kesl-control --get-settings 1 --file <vollständiger Dateipfad>
   ```

2. Öffnen Sie die erstellte Konfigurationsdatei zum Bearbeiten.

3. Fügen Sie der erstellten Datei folgenden Abschnitt hinzu:

   ```
   [ExcludedFromScanScope.item_<Elementnummer>]
   Path=/var/opt/kaspersky/klms
   ```

4. Wiederholen Sie den oben genannten Abschnitt für alle Mail-Agenten, die mit Kaspersky Anti-Virus für Linux Mail Server integriert wurden.

5. Um das temporäre Verzeichnis für Filter und Dienste von Kaspersky Anti-Virus für Linux Mail Server von der Untersuchung auszuschließen, fügen Sie der erstellten Datei folgenden Abschnitt hinzu:

   ```
   [ExcludedFromScanScope.item_<Elementnummer>]
   Path=/tmp/klmstmp
   ```

6. Speichern Sie die Änderungen in der Konfigurationsdatei.

7. Importieren Sie die Einstellungen aus der Konfigurationsdatei in die Aufgabe zum Schutz vor bedrohlichen Dateien mithilfe des folgenden Befehls:

   ```
   kesl-control --set-settings 1 --file <vollständiger Dateipfad>
   ```

Informationsquellen zu Kaspersky Endpoint Security

Seite für Kaspersky Endpoint Security in der Wissensdatenbank

Die Wissensdatenbank ist ein Abschnitt der Website des technischen Supports.

Auf der Seite von Kaspersky Endpoint Security in der Wissensdatenbank finden Sie nützliche Informationen, Tipps und Antworten auf häufig gestellte Fragen. Dabei werden Fragen wie Kauf, Installation und Verwendung der App behandelt.

Die Artikel der Wissensdatenbank behandeln neben Fragen zu Kaspersky Endpoint Security auch andere Apps von Kaspersky. Die Artikel in der Wissensdatenbank können auch Neuigkeiten des Technischen Supports enthalten.

Diskussion über Kaspersky-Apps im Forum

Wenn Ihre Frage nicht dringend ist, können Sie sie mit den Kaspersky-Experten und mit anderen Benutzern in unserem Forum diskutieren.

Im Forum können Sie Diskussionsthemen lesen, eigene Kommentare schreiben und neue Themen zur Diskussion stellen.

Glossar

Abonnement

Verwendung der App mit den ausgewählten Einstellungen (Enddatum, Anzahl der Geräte). Sie können ein Abonnement anhalten, fortsetzen, automatisch verlängern lassen oder kündigen.

Administrationsgruppe

Gruppe von Geräten, die aufgrund ihrer ausgeführten Funktionen und der darauf installierten Gruppe von Kaspersky-Apps in Kaspersky Security Center zusammengefasst wurden. Geräte werden zur bequemen Handhabung als Einheiten in Gruppen zusammengefasst. Eine Administrationsgruppe kann andere Gruppen beinhalten. Für alle in der Administrationsgruppe installierten Apps können Gruppenrichtlinien angelegt und Gruppenaufgaben erstellt werden.

Administrationsserver

Eine Komponente der App Kaspersky Security Center, die Informationen über alle Apps von Kaspersky, die innerhalb des Unternehmensnetzwerks installiert sind, zentral speichert und deren Verwaltung ermöglicht.

Aktive Richtlinie

Die Richtlinie, die von der App derzeit zur Vermeidung von Datenverlust verwendet wird. Die App kann mehrere Richtlinien gleichzeitig verwenden.

Aktiver Schlüssel

Ein Schlüssel, der momentan der App verwendet wird.

Anwendungseinstellungen

Einstellungen für die Ausführung der App, die für alle Aufgabentypen gleich sind und den Gesamtbetrieb der App regeln, zum Beispiel Leistungseinstellungen der App, Berichtseinstellungen und Backup-Einstellungen.

App aktivieren

Freischaltung aller Funktionen der App. Die App wird vom Benutzer während oder nach der Installation aktiviert. Für die Aktivierung der App benötigt der Benutzer einen Aktivierungscode oder eine Schlüsseldatei.

App-Datenbanken

Datenbanken, die Informationen über Bedrohungen der Computersicherheit enthalten, die Kaspersky zum Veröffentlichungsdatum der Datenbank bekannt waren. Die Datenbanken der App werden von Kaspersky-Experten erstellt und stündlich aktualisiert.

Ausschluss

Ein *Ausschluss* ist ein Objekt, das von der Untersuchung durch eine Kaspersky-App ausgeschlossen ist. Es können Dateien eines bestimmten Formats, Dateien nach Maske, ein bestimmter Bereich (z. B. ein Ordner oder ein Programm), Programmprozesse oder Objekte nach Namen gemäß der Klassifizierung der Viren-Enzyklopädie von der Untersuchung ausgeschlossen werden. Für jede Aufgabe können separate Ausschlüsse angegeben werden.

Autostart-Objekte

Bestimmte Apps, die für den Start und den korrekten Betrieb des auf Ihrem Computer installierten Betriebssystems und der Software erforderlich sind. Bei jedem Start des Betriebssystem werden diese Objekte gestartet. Es gibt Viren, die in der Lage sind, eben solche Objekte zu infizieren, was beispielsweise dazu führen kann, dass der Start des Betriebssystems blockiert wird.

Dateimaske

Platzhalter für den Namen einer Datei, der aus allgemeinen Zeichen besteht. Die wichtigsten Zeichen in Dateimasken sind * und ? (wobei * für eine beliebige Anzahl von Zeichen steht und ? für ein beliebiges Einzelzeichen).

Datenbank mit bösartigen Webadressen

Liste der Adressen von Webressourcen, deren Inhalt als gefährlich eingestuft werden kann. Die Liste wird von Kaspersky-Experten zusammengestellt, wird regelmäßig aktualisiert und gehört zum Lieferumfang der Kaspersky-App.

Datenbank mit Phishing-Webadressen

Liste der Adressen von Webressourcen, die von Kaspersky-Experten als Phishing identifiziert wurden. Die Datenbank wird regelmäßig aktualisiert und gehört zum Lieferumfang der Kaspersky-App.

Desinfektion von Objekten

Ein Verfahren zur Verarbeitung von infizierten Objekten, das zu einer vollständigen oder teilweisen Wiederherstellung von Daten führt. Nicht alle infizierten Objekte können desinfiziert werden.

Fehlalarm

Eine Situation, in der eine App von Kaspersky ein nicht infiziertes Objekt als infiziert betrachtet, weil dessen Code dem eines Virus ähnelt.

Gruppenaufgabe

Eine Aufgabe, die einer Administrationsgruppe zugewiesen ist und auf allen verwalteten Geräten innerhalb dieser Gruppe ausgeführt wird.

Gruppenrichtlinie

siehe Richtlinie.

Infiziertes Objekt

Ein Objekt mit einem Code-Fragment, welches vollständig mit dem Code-Fragment eines bekannten gefährlichen Programms übereinstimmt. Kaspersky-Experten empfehlen, solche Objekte nicht zu verwenden.

Integrationsserver

Die Komponente "Kaspersky Endpoint Security for Virtualization Light Agent". Realisiert die Interaktion zwischen den Komponenten von Kaspersky Endpoint Security und der virtuellen Infrastruktur.

Kaspersky-Update-Server

HTTP- und FTP-Server von Kaspersky, von denen die Apps Datenbanken-Updates und Updates von Modulen der App erhalten.

Light Agent

Die Komponente "Kaspersky Endpoint Security for Virtualization Light Agent". Wird auf jeder virtuellen Maschine installiert, die geschützt werden muss.

Lizenz

Ein zeitlich begrenztes Nutzungsrecht für eine App, das Ihnen auf Basis eines Endbenutzer-Lizenzvertrags überlassen wird.

Lizenzzertifikat

Ein Dokument, das Sie von Kaspersky zusammen mit der Schlüsseldatei oder dem Aktivierungscode erhalten. Dieses Dokument enthält Informationen über die bereitgestellte Lizenz.

Proxy-Server

Ein Netzwerkdienst, mit dem Clients indirekte Anfragen an andere Netzwerkdienste richten können. Der Client baut zunächst eine Verbindung zu einem Proxy-Server auf und fordert eine bestimmte Ressource an (z. B. eine Datei), die sich auf einem anderen Server befindet. Dann stellt der Proxy-Server entweder eine Verbindung zum angegebenen Server her und ruft die Ressource von dort ab, oder er gibt die Ressource aus dem eigenen Cache zurück (falls der Proxy-Server über einen eigenen Cache verfügt). In einigen Fällen kann die Client-Anfrage oder die Antwort des Servers für bestimmte Zwecke vom Proxy-Server verändert werden.

Reserveschlüssel

Ein Schlüssel, der das Recht auf Nutzung der App gewährt, jedoch im Augenblick nicht aktiviert ist.

Richtlinie

Eine Richtlinie bestimmt die Einstellungen für den Betrieb der App und verwaltet den Zugriff auf die Konfiguration von auf Geräten innerhalb einer Administrationsgruppe installierten Apps. Für jede App muss eine eigene Richtlinie erstellt werden. Sie können eine unbegrenzte Anzahl von unterschiedlichen Richtlinie für eine auf den Geräten der einzelnen Administrationsgruppen installierte App erstellen. Allerdings kann innerhalb einer Administrationsgruppe pro App nur eine Richtlinie gleichzeitig angewendet werden.

SIEM-System

Das *SIEM-System (Security Information and Event Management)* ist eine Lösung zur Verwaltung von Informationen und Ereignissen im Sicherheitssystem eines Unternehmens.

SVM

Eine Secure Virtual Machine (SVM) ist eine spezielle virtuelle Maschine, auf welcher der Dienst "scanserver" (Dienst des Schutzservers als Komponente von Kaspersky Security for Virtualization Light Agent) installiert ist.

Vertrauenswürdiges Gerät

Ein Gerät, auf das Benutzer, die in den Einstellungen des vertrauenswürdigen Geräts festgelegt wurden, jederzeit vollständigen Zugriff haben.

Informationen über den Code von Drittherstellern

Informationen über den Code von Drittherstellern finden Sie in der Datei legal_notices.txt, die sich im Installationsordner der App befindet.

Markeninformationen

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

Amazon ist ein Markenzeichen von Amazon.com, Inc. oder seinen verbundenen Unternehmen.

FireWire ist eine Markenzeichen von Apple Inc.

Arm ist ein eingetragenes Markenzeichen von Arm Limited (oder seinen Tochtergesellschaften) in den Vereinigten Staaten und/oder anderen Ländern.

Die Bluetooth-Wortmarke, das Markenzeichen und die Bluetooth-Logos sind Eigentum von Bluetooth SIG, Inc.

Ubuntu und LTS sind eingetragene Markenzeichen von Canonical Ltd.

Citrix und XenServer sind Markenzeichen von Citrix Systems, Inc. und/oder Tochterunternehmen, die bei den Patentämtern in den USA uns in anderen Ländern registriert sind.

Cloudflare, das Cloudflare-Logo und Cloudflare Workers sind Markenzeichen und/oder eingetragene Markenzeichen von Cloudflare, Inc. in den USA und anderen Jurisdiktionen.

Docker und das Docker-Logo sind Markenzeichen oder eingetragene Markenzeichen von Docker, Inc. in den USA und/oder anderen Ländern. Docker Inc. und andere Parteien haben möglicherweise auch Markenrechte, die durch andere in diesem Dokument verwendete Begriffe beschrieben werden.

Chrome und Google Public DNS sind Markenzeichen von Google LLC.

HUAWEI, EulerOS und FusionSphere sind Markenzeichen der Huawei Technologies Co., Ltd.

Intel und Core sind eingetragene Markenzeichen der Intel Corporation in den USA und/oder in anderen Ländern.

Linux ist ein in den USA und/oder in anderen Ländern eingetragenes Markenzeichen von Linus Torvalds.

Microsoft, Active Directory, Hyper-V, Outlook, Visual C++ und Windows sind eingetragene Markenzeichen der Microsoft-Unternehmensgruppe.

OpenStack ist ein eingetragenes Markenzeichen der OpenStack Foundation in den USA und anderen Ländern.

Oracle und JavaScript sind eingetragene Markenzeichen des Unternehmens Oracle und/oder von verbundenen Unternehmen.

Red Hat, Red Hat Enterprise Linux und CentOS sind Markenzeichen und/oder sind in den USA und anderen Ländern eingetragene Markenzeichen von Red Hat, Inc. oder seinen Tochterunternehmen.

Debian ist eine registrierte Marke von Software in the Public Interest, Inc.

SUSE ist eine in den USA und in anderen Ländern eingetragene Marke von SUSE LLC.

Mware, VMware NSX, VMware NSX Manager, VMware Tools, VMware vCenter und VMware vSphere sind Markenzeichen VMWare, Inc. oder in den USA und in anderen Ländern eingetragene Markenzeichen.

UNIX ist eine in den USA und in anderen Ländern eingetragene Marke; ihre Nutzung wird von X/Open Company Limited lizenziert.