kaspersky

Kaspersky Endpoint Security für Linux 12.5.0

© 2026 AO Kaspersky Lab

Inhalt

Kaspersky Endpoint Security für Linux
Über das Programm
- Wichtige Funktionen
- Neuerungen in Version 12.5
- Behobene Probleme
- Hard- und Softwarevoraussetzungen
- Lieferumfang
- Kompatibilität mit anderen Programmen
- Vergleich des Funktionsumfangs verschiedener Kaspersky-Lösungen

Bereitstellung und Erstkonfiguration
- Modi und Bereitstellungsschemata
- Umgebung für die Programminstallation vorbereiten
- Auswahl des Mechanismus zum Abfangen von Systemereignissen
- Programmpakete vorbereiten
- Vorbereitende Aktionen in Kaspersky Security Center
- Das Programm mithilfe von Kaspersky Security Center installieren
- Anwendung über die Befehlszeile installieren
- Zusätzliche Konfigurationsschritte nach der Installation in bestimmten Betriebssystemen
- Migrationsszenario zu Kaspersky Security Center für Linux mithilfe des Schnellinstallationsskripts
- Update einer Vorgängerversion der Anwendung durchführen
  - Informationen zum Aktualisieren der Verwaltungs-Plug-ins für Kaspersky Endpoint Security
  - Programmeinstellungen nach dem Upgrade
- Anwendung deinstallieren

Verwenden der App
- Lizenzverwaltung
  - So wechseln Sie zu einer anderen Kaspersky-Lösung
  - Lizenzschlüssel verwalten
  - Informationen zu Lizenzschlüsseln anzeigen
- Verwaltungsschnittstellen der App
  - App mithilfe von Kaspersky Security Center verwalten
    - Über die Richtlinien von Kaspersky Security Center
    - Richtlinienverwaltung
    - Exportieren und Importieren von Richtlinieneinstellungen
    - Über die Aufgaben für Kaspersky Endpoint Security, die in Kaspersky Security Center erstellt wurden
    - An Web Console und Cloud Console an- und abmelden
  - App über die Befehlszeile verwalten
    - Lokale Aufgaben von Kaspersky Endpoint Security
    - Aufgabenparameter ändern
    - Zeitplan für Aufgaben konfigurieren
    - Allgemeine App-Einstellungen verwalten
    - Filter zur Eingrenzung der Abfrageergebnisse verwenden
    - Anwendungseinstellungen exportieren und importieren
  - Verwaltung der Anwendung über die grafische Benutzeroberfläche

Überwachung des Schutzstatus
- Echtzeit-Schutzstatus
- Ereignisse und Berichte
  - Protokollierung von Ereignissen im Protokoll des Betriebssystems konfigurieren
  - Einstellungen des Ereignisprotokolls der Anwendung konfigurieren
  - Programmereignisse anzeigen
  - Berichte anzeigen
- Kennzahlen zum Systemzustand sammeln
- Überwachung der Anwendungsstabilität
- Integritätsprüfung der Anwendungskomponenten

Zugriffssteuerung für Apps
- Vordefinierte Rollen
- Benutzerrolle zuweisen oder entziehen
- RBAC-Funktionsbereiche in Kaspersky Security Center

Empfehlungen für typische Rollen geschützter Geräte

Datenbanken und Module des Programms aktualisieren
- Auswählen der Update-Quelle und des Verteilungsschemas
- Aufgabe zum Datenbanken-Update konfigurieren
- So aktualisieren Sie mithilfe von Kaspersky Update Utility
- So führen Sie ein Rollback für Updates der Programmdatenbanken und -module durch

Geräteschutz vor Bedrohungen
- Schutz vor bedrohlichen Dateien
  - So erstellen Sie einen Schutzbereich
  - So wählen Sie eine Aktion beim Erkennen einer Dateibedrohung aus
  - Was ist der intelligente Modus der Dateiuntersuchung?
  - So optimieren Sie die Untersuchung von Dateien
  - Besonderheiten der Untersuchung von symbolischen Links und festen Links
- Schadsoftware-Untersuchung.
  - So erstellen Sie einen Untersuchungsbereich
  - So konfigurieren Sie einen Untersuchungszeitplan
  - So untersuchen Sie eine einzelne Datei oder ein Verzeichnis
  - So optimieren Sie Aufgaben zur benutzerdefinierten Untersuchung
- Untersuchung wichtiger Bereiche.
- Container untersuchen
  - So konfigurieren Sie die Integration mit Tools zur Containerverwaltung
  - So erstellen Sie einen Untersuchungsbereich für die Untersuchung von Containern und Images auf Befehl
  - So optimieren Sie die Untersuchung von Containern
  - So wählen Sie eine Aktion aus, die beim Fund eines infizierten Objekts für einen Container ausgeführt werden soll
  - So führen Sie eine benutzerdefinierte Untersuchung von Containern und Images aus
- Untersuchung von Wechseldatenträgern
- Verhaltensanalyse
- Exploit-Prävention
- Schutz vor Verschlüsselung
  - Aktion beim Fund bösartiger Verschlüsselung auswählen
  - So erstellen Sie einen Schutzbereich

- Schutz vor modifizierten USB-Geräten
  - So konfigurieren Sie die Autorisierung von USB-Geräten
  - So erlauben Sie das Anschließen von USB-Geräten mithilfe der Bildschirmtastatur
  - So erlauben Sie das Anschließen von USB-Geräten mithilfe des Barcode-Scanners
- Schutz von Verbindungen und Kommunikation über das Netzwerk
  - Schutz vor E-Mail-Bedrohungen
    - Was ist zu tun, wenn eine E-Mail-Bedrohung erkannt wird
    - So optimieren Sie die Untersuchung von E-Mail-Anhängen
    - Wozu ein Filter für E-Mail-Anhänge dient
  - Schutz vor Web-Bedrohungen
    - Aktion beim Fund einer Web-Bedrohung auswählen
    - Was ist Anti-Phishing
  - Schutz vor Netzwerkbedrohungen
    - So wählen Sie eine Aktion bei der Erkennung von Netzwerkbedrohungen aus
    - Blockierte Geräte verwalten
  - Firewall-Verwaltung
    - So erstellen Sie eine Regel für Netzwerkpakete
    - Beispiele für die Verwendung von Regeln für Netzwerkpakete
    - So fügen Sie einer Netzwerkzone eine IP-Adresse hinzu: Öffentlich, Lokal, Vertrauenswürdig
    - Was sind dynamische Regeln?
    - So erstellen Sie Regeln für die Verbindung mit Kaspersky Security Center
- Sicherheitskontrolle
  - Gerätekontrolle
    - So verwalten Sie die Liste der vertrauenswürdigen Geräte über die Befehlszeile
    - Zugriffsmodus für Geräte konfigurieren
    - Gerätezugriffsregeln konfigurieren
    - So konfigurieren Sie die Nachrichtenvorlage der Gerätekontrolle
    - Temporären Zugriff auf das Gerät gewähren
  - Web-Kontrolle
    - So erstellen Sie eine Zugriffsregel für Webressourcen
    - So ändern Sie Nachrichtenvorlagen der Web-Kontrolle
    - Regeln zum Definieren von Adressmasken für Webressourcen
  - Programmkontrolle
    - Programminventarisierung
    - So konfigurieren Sie den Betriebsmodus der Programmkontrolle
    - Programmkategorien erstellen
    - Golden Image
    - Über die Regeln für die Programmkontrolle
    - Testmodus für Regeln der Programmkontrolle
  - Überwachung der System-Integrität
    - Überwachung der Systemintegrität in Echtzeit
    - Prüfung der Systemintegrität
- Vertrauenswürdige Zone
  - So fügen Sie Schutzausnahmen hinzu
  - So fügen Sie vertrauenswürdige Webadressen hinzu
  - So fügen Sie eine vertrauenswürdige IP-Adresse eines Computers hinzu
  - So wählen Sie überwachte Netzwerkports aus

- So fügen Sie ein Zertifikat zur Liste der vertrauenswürdigen Stammzertifikate hinzu
- So fügen Sie eine vertrauenswürdige Domäne hinzu
- So schließen Sie Mount-Punkte aus
- So fügen Sie vertrauenswürdige Programme hinzu
- So fügen Sie vertrauenswürdige Geräte hinzu

Allgemeine Einstellungen

- Konfiguration der Erkennung
- Kaspersky Security Network
  - So aktivieren oder deaktivieren Sie Kaspersky Security Network
  - Was ist der Cloud-Modus des Programms
  - Wozu dient der KSN-Proxy
- Übertragung von Informationen an den Speicher von Kaspersky Security Center konfigurieren
- So konfigurieren Sie den Programmstart
- Berechtigungen für die Aufgabenverwaltung konfigurieren
- Kennwortschutz
  - Über benutzerdefinierte Berechtigungen
  - Standardmäßige Benutzerberechtigungen
- Leistungseinstellungen
- Netzwerkeinstellungen
  - So verwalten Sie die Proxy-Einstellungen
  - So fängt das Programm den Datenverkehr ab
  - So konfigurieren Sie die Richtlinie zur Zertifikatsvalidierung
  - So konfigurieren Sie überwachte Ports
  - Ausnahmen vom Abfangen des Datenverkehrs durch Tools des Betriebssystems
- Überwachung von Dateioperationen
- Abfangen von Systemereignissen konfigurieren
- Erweiterte Einstellungen für Telemetriedaten konfigurieren
- Datenverwaltung

Schutz vor komplexen Bedrohungen und gezielten Angriffen

- Reaktionsaktionen
  - IOC-Untersuchung
  - Netzwerkisolation
    - Netzwerkisolation eines Geräts manuell in der Web Console aktivieren und deaktivieren
    - Dauer der Netzwerkisolation im automatischen Modus konfigurieren
    - Parameter der Netzwerkisolation manuell einrichten
    - Ausnahmen von der Netzwerkisolation in der Web Console konfigurieren
  - Die Datei in die Quarantäne verschieben.
  - Datei von Gerät abrufen
  - Datei von Gerät löschen
  - Einen Prozess starten
  - Eines Prozesses beenden
  - Ausführungsprävention für Objekte
  - Quarantäne verwenden
- Endpoint Detection and Response Optimum
  - So aktivieren Sie die Integration mit EDR Optimum
  - So überprüfen Sie, ob die EDR Optimum-Integration ordnungsgemäß funktioniert
  - Cloud Sandbox

- Endpoint Detection and Response Expert (On-Premises)
  - So bereiten Sie ein Referenzabbild für die korrekte Integration mit EDR Expert (on-premises) vor
  - So konfigurieren Sie die Integration von EDR Expert (on-premise)
  - So überprüfen Sie, ob die Integration in EDR Expert (on-premise) betriebsbereit ist
- Endpoint Detection and Response Expert (cloud)
  - So konfigurieren Sie die Integration des integrierten Agenten in EDR Expert (cloud)
  - So optimieren Sie die Übertragung von Telemetriedaten in EDR Expert (cloud)
  - So konfigurieren Sie Ausnahmen für Telemetriedaten in EDR Expert (cloud)
  - So exportieren oder importieren Sie Ereignisfilter für EDR Expert (cloud)
- Kaspersky Anti Targeted Attack Platform
  - So konfigurieren Sie die EDR (KATA)-Integration
  - So konfigurieren Sie die NDR (KATA)-Integration
  - So überprüfen Sie, ob die KATA-Integration ausgeführt wird
- Sandbox
  - So konfigurieren Sie die Integration mit Sandbox
  - So überprüfen Sie, ob die Integration mit Sandbox ausgeführt wird
  - So senden Sie eine Datei manuell an Sandbox
- Kaspersky Managed Detection and Response
  - Empfehlungen zum Erstellen eines Referenzabbilds für die korrekte Integration mit MDR
  - Hochladen der KPSN-Konfigurationsdatei
  - MDR-Integration konfigurieren
  - Überprüfen, ob die MDR-Integration aktiviert ist
- Kaspersky Unified Monitoring and Analysis Platform
  - KUMA-Integration konfigurieren
  - So überprüfen Sie, ob die KUMA-Integration ausgeführt wird

- Schutz virtueller Umgebungen
  - So konfigurieren Sie die SVM-Erkennung
  - Wie Light Agent SVMs auswählt
  - So verteilen Sie die Verbindungen von Light Agents auf SVMs
  - Schutz der Verbindung zwischen Light Agent und einer SVM
  - So ermitteln Sie den Status des Light Agent

Bewährte Methoden

- Optimierung der Ressourcenauslastung durch die Anwendung
  - Nutzung der Geräteressourcen durch die Anwendung analysieren
  - Empfehlungen für den Schutz vor bedrohlichen Dateien und die Untersuchungsaufgaben
  - Empfehlungen für den Schutz vor Web-Bedrohungen und den Schutz vor Netzwerkbedrohungen
  - Empfehlungen für die Verhaltensanalyse
- Interoperabilität mit Kaspersky-Lösungen
  - Kaspersky Security Center Linux
  - Kaspersky Unified Monitoring and Analysis Platform

Referenz zu den Programmkomponenten

- Befehle zur Verwaltung von Kaspersky Endpoint Security
  - Befehle zur Verwaltung der Lizenzschlüssel
  - Befehle zur Verwaltung von Benutzern und Rollen
  - Verwalten von App-Aufgaben und -Einstellungen
    - Befehle zur Verwaltung der allgemeinen Anwendungseinstellungen
    - Befehle zur Verwaltung der Aufgabeneinstellungen

Befehle zur Aufgabenverwaltung
Befehle zur Verwaltung der allgemeinen Einstellungen für die Untersuchung von Containern
Befehle zur Verwaltung der Einstellungen für die Untersuchung des Netzwerkverkehrs
Status- und Schutzüberwachung
Statistikbefehle
Befehl zur Anzeige von Ereignissen
Befehle zur Verwaltung der Ereignisse der Anwendung
Befehl zum Verwalten von Systemleistungsmetriken
Sicherheitskontrolle
Befehle zur Verwaltung der Gerätekontrolle
Befehle zur Verwaltung der Programmkontrolle
Befehle zur Verwaltung der Web-Kontrolle
Schutz von Netzwerkverbindungen
Befehle zur Verwaltung blockierter Geräte
Befehle zur Firewall-Verwaltung
Schutz vor komplexen Bedrohungen und gezielten Angriffen
Befehle zur Verwaltung der Quarantäne
Befehle zur Verwaltung der Komponente EDR Expert (on-premise)
Befehle zur Verwaltung der Komponente EDR Expert (cloud)
Befehle zur Verwaltung von NDR (KATA)
Befehle zur Verwaltung der Netzwerkisolation eines Geräts
Befehle zur Verwaltung der Integrationseinstellungen für KUMA
Befehle zur Verwaltung der Integrationseinstellungen für Sandbox
Befehle zur Verwaltung der IOC-Untersuchung
Programmbefehle im Light Agent-Modus
Befehlszeilenoptionen des Programms
Update-Aufgabe
Geräteschutz vor Bedrohungen
Aufgabe zum Schutz vor bedrohlichen Dateien
Optimierung der Überprüfung von Netzwerkverzeichnissen
Schadsoftware-Untersuchung
Aufgabe zur Schadsoftware-Untersuchung
Aufgabe zur benutzerdefinierten Untersuchung
Aufgabe zur Untersuchung wichtiger Bereiche
Aufgabe „Untersuchung von Wechseldatenträgern“
Container untersuchen
Einstellungen der Untersuchung von Containern
Aufgabe zur Untersuchung von Containern
Integration mit Jenkins
Aufgabe zum Schutz vor Verschlüsselung
Aufgabe zur Verhaltensanalyse
Exploit-Prävention
Arbeiten mit dem Kaspersky Security Network
Verbindung mit Kaspersky Security Network herstellen
Aktivieren oder Deaktivieren des Cloud-Modus
Aufgabe zum Schutz vor BadUSB-Angriffen

Schutz von Verbindungen und Kommunikation über das Netzwerk
Aufgabe zum Schutz vor Web-Bedrohungen
Netzwerkverkehr untersuchen
Einstellungen zur Untersuchung des Netzwerkverkehrs anzeigen und ändern
Ausschlüsse von der Untersuchung verschlüsselter Verbindungen anzeigen
Liste der vertrauenswürdigen Stammzertifikate verwalten
Ausnahmen vom Abfangen des Datenverkehrs konfigurieren und anzeigen
Aufgabe zum Schutz vor Netzwerkbedrohungen
Firewall-Verwaltung
Konfigurieren der Liste der Regeln für Netzwerkpakete
Konfigurieren von Netzwerkzonen
Sicherheitskontrolle
Aufgabe zur Gerätekontrolle
Web-Kontrolle
Aufgabe „Web-Kontrolle“
Einstellungen der Web-Kontrolle anzeigen und ändern
Programmkontrolle
Aufgabe zur Programmkontrolle
Eine Liste mit Kategorien erstellen und bearbeiten
Eine Liste mit Kategorien anzeigen
Einstellung der Liste mit Regeln für die Programmkontrolle
Inventarisierung konfigurieren
Inventarisierungsaufgabe
Liste der gefundenen Apps anzeigen
Aufgabe zur Überwachung der Systemintegrität
Aufgabe zur Prüfung der Systemintegrität
Schutz vor komplexen Bedrohungen und gezielten Angriffen
Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)
Einstellungen der Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)
Verwaltung der Zertifikate für die Verbindung mit OSMP EDR Expert (on-premise)-Servern
Integration mit Kaspersky Endpoint Detection and Response Expert (cloud)
Integrationseinstellungen für Kaspersky Endpoint Detection and Response Expert (cloud)
Verwalten von Verbindungszertifikaten für OSMP EDR Expert-Server (cloud)
Integration mit Kaspersky Endpoint Detection and Response (KATA)
Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA)
Zertifikate für die Verbindung mit dem KATA-Server verwalten
Integration mit Kaspersky Network Detection and Response (KATA)
Parameter für die Integration mit Kaspersky Network Detection and Response (KATA)
Zertifikate für die Verbindung mit dem NDR-Server verwalten
Integration mit Sandbox
Einstellungen für die Integration mit Sandbox
Verwaltung der Zertifikate für die Verbindung mit dem Sandbox-Server
Integration mit Kaspersky Endpoint Detection and Response Optimum aktivieren und deaktivieren
Konfigurieren der Integration von Kaspersky Managed Detection and Response
Verwalten der Netzwerkisolation von Geräten
Parameter der Quarantäne konfigurieren
Quarantäne-Dateien über die Befehlszeile verwalten

IOC-Untersuchung
Verwaltung der Ausführungsprävention
Konfiguration der KUMA-Integration
Aufgabe zur Integration mit Kaspersky Unified Monitoring and Analysis Platform
Zertifikate für die Verbindung mit dem KUMA-Server verwalten
Allgemeine Einstellungen
Allgemeine Anwendungseinstellungen
Aufgabenzeitplan
Einstellungen für Proxyserver
Backup-Einstellungen konfigurieren
Einstellungen der Untersuchung des Netzwerkdatenverkehrs
Globale Ausschlüsse konfigurieren
Einstellungen für den Kennwortschutz
Programmeinstellungen in der Verwaltungskonsole
Datenbanken-Update
Geräteschutz vor Bedrohungen
Komponente "Schutz vor bedrohlichen Dateien".
Fenster "Untersuchungsbereiche"
Fenster „Neuer Untersuchungsbereich“
Fenster "Untersuchungseinstellungen"
Fenster "Aktionen beim Erkennen von Bedrohungen"
Ausschlüsse aus dem Schutz vor bedrohlichen Dateien
Fenster "Ausschlussbereiche"
Fenster „Neuer Ausnahmebereich“
Fenster "Ausnahmen nach Maske"
Fenster "Ausschlüsse nach Bedrohungsname"
Fenster "Ausnahmen nach Prozess"
Fenster "Vertrauenswürdiger Prozess"
Schadsoftware-Untersuchung
Fenster "Untersuchungsbereiche"
Fenster <Neuer Untersuchungsbereich>
Fenster "Einstellungen des Untersuchungsbereichs"
Fenster "Untersuchungsbereiche"
Fenster "Untersuchungseinstellungen"
Fenster "Aktionen beim Erkennen von Bedrohungen"
Abschnitt "Ausnahmen"
Fenster "Ausschlussbereiche"
Fenster „Neuer Ausnahmebereich“
Fenster "Ausnahmen nach Maske"
Fenster "Ausschlüsse nach Bedrohungsname"
Untersuchung wichtiger Bereiche
Fenster "Untersuchungsbereiche"
Fenster „Neuer Untersuchungsbereich“
Fenster "Einstellungen des Untersuchungsbereichs"
Fenster "Untersuchungsbereiche"
Fenster "Untersuchungseinstellungen"
Fenster "Aktionen beim Erkennen von Bedrohungen"

- Abschnitt "Ausnahmen"
- Fenster "Ausschlussbereiche"
- Fenster „Neuer Ausnahmebereich“
- Fenster "Ausnahmen nach Maske"
- Fenster "Ausschlüsse nach Bedrohungsname"
- Container-Überwachung
  - Fenster "Einstellungen der Container-Untersuchung"
- Container untersuchen
  - Fenster "Einstellungen der Container-Untersuchung"
  - Fenster "Untersuchungseinstellungen"
  - Fenster "Aktionen beim Erkennen von Bedrohungen"
  - Abschnitt "Ausnahmen"
  - Fenster "Ausnahmen nach Maske"
  - Fenster "Ausschlüsse nach Bedrohungsname"
- Untersuchung von Wechseldatenträgern
- Verhaltensanalyse
  - Fenster "Ausnahmen nach Prozess"
  - Fenster "Vertrauenswürdiger Prozess"
- Exploit-Prävention
  - Fenster "Ausnahmen aus der Exploit-Prävention"
  - Fenster "Ausnahme aus der Exploit-Prävention"
- Schutz vor Verschlüsselung
  - Fenster "Untersuchungsbereiche"
  - Fenster „Neuer Untersuchungsbereich“
  - Fenster "Schutzeinstellungen"
  - Fenster "Ausschlussbereiche"
  - Fenster „Neuer Ausnahmebereich“
  - Fenster "Ausnahmen nach Maske"
- Kaspersky Security Network
  - Einstellungen für „Kaspersky Security Network“
  - Erklärung zu Kaspersky Security Network
  - Erklärung zu Kaspersky Private Security Network
- Schutz vor modifizierten USB-Geräten

Schutz von Verbindungen und Kommunikation über das Netzwerk

- Schutz vor E-Mail-Bedrohungen
  - Fenster "Einstellungen des Schutzes vor E-Mail-Bedrohungen"
  - Fenster "Anhangsfilter"
- Schutz vor Web-Bedrohungen
  - Fenster "Vertrauenswürdige Webadressen"
  - Fenster "Untersuchungseinstellungen"
- Schutz vor Netzwerkbedrohungen
  - Fenster "Ausnahmen"
- Firewall-Verwaltung
  - Fenster "Regeln für Netzwerkpakete"
  - Fenster "Netzwerkpaketregel hinzufügen"
  - Fenster "IP-Adressen hinzufügen"

- Fenster "Verfügbare Netzwerke"
- Fenster "Netzwerkverbindung"

Sicherheitskontrolle

- Gerätekontrolle
  - Fenster Vertrauenswürdige Geräte
  - Fenster "Vertrauenswürdiges Gerät (Geräte-ID)"
  - Fenster "Geräte an Client-Geräten"
  - Fenster "Liste von Geräten basierend auf den Ereignissen der Gerätekontrolle"
  - Fenster "Zugriff auf ein vertrauenswürdiges Gerät"
  - Fenster "Benutzer oder Gruppe"
  - Fenster "Gerätetyp"
  - Fenster "Konfiguration der Gerätezugriffsregel"
  - Fenster "Benutzer oder Gruppe"
  - Fenster "Zugriffszeitplan"
  - Fenster "Verbindungsbusse"
- Web-Kontrolle
  - Fenster "Regel der Web-Kontrolle"
  - Fenster "Inhaltskategorien auswählen"
  - Fenster "Datentypkategorien auswählen"
  - Fenster "Adressen auswählen"
  - Fenster "Adressgruppen auswählen"
  - Fenster "Adressgruppe hinzufügen"
  - Fenster "Benutzer auswählen"
  - Fenster "Benutzer oder Gruppe"
  - Fenster "Zugriffszeitplan"
- Programmkontrolle
  - Fenster "Regeln der App-Kontrolle"
  - Fenster "Regel hinzufügen"
  - Fenster "Programmkategorien"
  - Fenster "Benutzer oder Gruppe"
  - Inventar
    - Fenster "Untersuchungsbereiche"
    - Fenster „Neuer Untersuchungsbereich“
    - Abschnitt "Ausnahmen"
    - Fenster "Ausschlussbereiche"
    - Fenster „Neuer Ausnahmebereich“
- Überwachung der System-Integrität
  - Fenster "Untersuchungsbereiche"
  - Fenster „Neuer Untersuchungsbereich“
  - Fenster "Ausschlussbereiche"
  - Fenster „Neuer Ausnahmebereich“
  - Fenster "Ausnahmen nach Maske"
  - Prüfung der Systemintegrität
    - Fenster "Untersuchungsbereiche"
    - Fenster „Neuer Untersuchungsbereich“
    - Abschnitt "Ausnahmen"
    - Fenster "Ausschlussbereiche"

Fenster „Neuer Ausnahmebereich“
Fenster "Ausnahmen nach Maske"
Lokale Aufgaben
Aufgabenverwaltung
Schutz vor komplexen Bedrohungen und gezielten Angriffen
Integration von Kaspersky Managed Detection and Response
Integration in Kaspersky Endpoint Detection and Response (on-premises)
Verbindung mit den KATA-Servern konfigurieren
Allgemeine Einstellungen für die Verbindung mit KATA-Servern konfigurieren
Datenübertragung an die KATA-Server konfigurieren
Integration mit Kaspersky Network Detection and Response (KATA)
Verbindung mit den NDR-Servern konfigurieren
Allgemeine Einstellungen für die Verbindung mit NDR-Servern konfigurieren
Datenübertragung an die NDR-Server konfigurieren
Integration mit KUMA
Fenster "KUMA-Server" (mehrere)
Fenster "KUMA-Server"
Fenster "Einstellungen für die Verbindung mit den KUMA-Servern"
Fenster zum Hinzufügen eines Serverzertifikats
Fenster zum Hinzufügen eines Client-Zertifikats
Quarantäne
Ausführungsprävention für Objekte
Allgemeine Einstellungen
Proxy-Server
Fenster "Proxyserver-Ausnahmen"
CPU-Auslastung durch Untersuchungsaufgaben
Ausführen von Aufgaben im Akkubetrieb
App starten
Automatischer Neustart, wenn ein kritisches Update empfangen wird
Kennwortschutz
Trace- und Dump-Einstellungen
Von der Anwendung genutzter residenter Speicher
Untersuchung verschlüsselter Verbindungen
Fenster "Vertrauenswürdige Domänen"
Fenster "Vertrauenswürdige Zertifikate"
Fenster "Ausnahmen vom Abfangen des Datenverkehrs"
Fenster "Ausnahme vom Abfangen des Datenverkehrs"
Fenster "Überwachte Ports"
Globale Ausnahmen
Fenster "Pfad zum Mountpunkt"
Ausschließen des Prozessspeichers von Untersuchungen
Datenverwaltung
Erkennen von Anwendungen, die von Angreifern für Kompromittierungen ausgenutzt werden können
Überwachung von Dateioperationen
Senden von Informationen an den Speicher von Kaspersky Security Center
Abfangen von Systemereignissen
Erweiterte Einstellungen zur Erfassung von Telemetriedaten

Light Agent-Modus
Verbindung zum Integrationsserver
Fenster "Verbindung zum Integrationsserver"
Fenster "Prüfung des Integrationsserver-Zertifikats"
Fenster "Authentifizierung auf dem Integrationsserver"
Einstellungen der SVM-Erkennung
Tag für die Verbindung zur SVM
Algorithmus der SVM-Auswahl
Schutz der Verbindung
Bekannte Probleme und Einschränkungen
Anfrage an den Technischen Support
Technischer Support über Kaspersky CompanyAccount
Informationen für den Technischen Support abrufen
So aktivieren und konfigurieren Sie die Erstellung von Protokolldateien
So aktivieren und konfigurieren Sie die Erstellung von Dump-Dateien
Ferndiagnose von Geräten mithilfe von Kaspersky Security Center
Anwendungen
Anhang 1. Konfigurationsdateien und Standardeinstellungen der App
Regeln zum Ändern von Konfigurationsdateien für die Aufgaben der Anwendung
Konfigurationsdateien für die Erstkonfiguration
Einstellungen für die Erstkonfiguration im Installationspaket
Vorinstallierte Konfigurationsdateien
Standardeinstellungen der Befehlszeilenaufgaben
Standardeinstellungen der Aufgabe File_Threat_Protection (ID:1)
Standardeinstellungen der Aufgabe Scan_My_Computer (ID:2)
Standardeinstellungen der Aufgabe Scan_File (ID:3)
Standardeinstellungen der Aufgabe Critical_Areas_Scan (ID:4)
Standardeinstellungen der Aufgabe Update (ID:6)
Standardeinstellungen der Aufgabe System_Integrity_Monitoring (ID:11)
Standardeinstellungen der Aufgabe Firewall_Management (ID:12)
Standardeinstellungen der Aufgabe Anti_Cryptor (ID:13)
Standardeinstellungen der Aufgabe Web_Threat_Protection (ID:14)
Standardeinstellungen der Aufgabe Device_Control (ID:15)
Standardeinstellungen der Aufgabe Removable_Drives_Scan (ID:16)
Standardeinstellungen der Aufgabe Network_Threat_Protection (ID:17)
Standardeinstellungen der Aufgaben Container_Scan (ID:18) und Custom_Container_Scan (ID:19)
Standardeinstellungen der Aufgabe Behavior_Detection (ID:20)
Standardeinstellungen der Aufgabe Application_Control (ID:21)
Standardeinstellungen der Aufgabe Inventory_Scan (ID:22)
Standardeinstellungen der Aufgabe KATAEDR (ID:24)
Standardeinstellungen der Aufgabe Web_Control (ID:26)
Standardeinstellungen der Aufgabe Standalone_Sandbox (ID:29)
Standardeinstellungen der Aufgabe KATANDR (ID:31)
Standardeinstellungen der Aufgabe KUMA (ID:33)
Standardeinstellungen für die Aufgabe zum Schutz vor E-Mail-Bedrohungen (ID: 35)
Standardeinstellungen für die Aufgabe zum Schutz vor BadUSB-Angriffen (ID: 37)
Standardeinstellungen der Aufgabe KATANDR (ID:31)

Anhang 2. Einstellungen für die Zusammenarbeit mit Kaspersky Anti-Virus für Linux Mail Server
Anhang 3. Parameter für die Interaktion mit externen Diensten
Anhang 4. Dateierweiterungen für die schnelle Untersuchung von Wechseldatenträgern
Anhang 5. Variablen in Nachrichtenvorlagen
Anhang 6. Programmereignisse
Kritisch
Warnung
Informative Meldung
Anhang 7. Rückgabecodes
Anhang 8. Archiv mit Programmdatenbanken vorbereiten
Anhang 9. Anforderungen an IOC-Dateien
Rechtliche Hinweise
Bereitstellung von Daten
Daten, die bei Verwendung eines Aktivierungscodes bereitgestellt werden
Daten, die beim Herunterladen von Updates von den Kaspersky-Update-Servern bereitgestellt werden
Daten, die bei Verwendung der Anwendung im Light Agent-Modus übertragen werden
Daten, die von der Anwendung an Kaspersky Security Center übertragen werden
Daten, die beim Klicken auf Links in der Oberfläche der Anwendung bereitgestellt werden
Daten, die bei der Verwendung von Kaspersky Security Network bereitgestellt werden
Daten, die bei der Integration mit der Lösung "Kaspersky Endpoint Detection and Response Optimum" bereitgestellt werden
Daten, die bei der Integration mit der Komponente "Kaspersky Endpoint Detection and Response (KATA)" bereitgestellt werden
Daten, die bei der Integration mit der Komponente "Kaspersky Endpoint Detection and Response Expert (on-premise)" bereitgestellt werden
Daten, die bei der Integration mit der Komponente Kaspersky Endpoint Detection and Response Expert (cloud) bereitgestellt werden
Daten, die bei der Integration mit der Komponente "Kaspersky Network Detection and Response (KATA)" bereitgestellt werden
Daten, die bei der Integration mit der Lösung "Kaspersky Unified Monitoring and Analysis Platform" bereitgestellt werden
Informationen über den Code von Drittherstellern
Markenrechtliche Hinweise

Kaspersky Endpoint Security für Linux

Durchsuchen

Kaspersky Endpoint Security für Linux
Neuerungen in Version 12.5
Typische Bereitstellungsschemata
Funktionsvergleich
Bekannte Probleme und Einschränkungen

Schnellstart

Hardware- und Softwarevoraussetzungen
Kompatibilität
Programmpakete vorbereiten
Umgebung für die Installation vorbereiten
Anwendung bereitstellen
Migrationsszenario zu Kaspersky Security Center Linux

Verwenden der Anwendung

Aktivierung
Datenbanken aktualisieren
Update mithilfe von Kaspersky Update Utility
Schutz vor bedrohlichen Dateien
Vertrauenswürdige Zone
Ressourcen optimieren

Konfigurieren in der Befehlszeile

Anwendung über die Befehlszeile verwalten
Verwaltungsbefehle
Befehlszeilenoptionen des Programms

Support

Überwachung des Schutzstatus
Upgrade einer älteren Programmversion
Kontaktaufnahme mit dem Technischen Support

Über das Programm

Kaspersky Endpoint Security für Linux bietet einen erweiterten, umfassenden Schutz für Linux-Geräte und ermöglicht es, verschiedene Arten von Bedrohungen, Netzwerkangriffen und Betrug zu verhindern, zu erkennen und darauf zu reagieren. Das Programm ist in vielen plattformübergreifenden Lösungen von Kaspersky enthalten und kann flexibel an die Herausforderungen der IT-Infrastruktur Ihres Unternehmens angepasst werden.

Sie können Kaspersky Endpoint Security, das auf geschützten Geräten installiert ist, sowohl lokal als auch zentral mithilfe von Kaspersky Security Center verwalten.

Die Anwendung ist nicht für den Einsatz im Rahmen technologischer Prozesse vorgesehen, die automatisierte Steuerungssysteme verwenden. Um Geräte in solchen Umgebungen zu schützen, wird es empfohlen, stattdessen die Anwendung Kaspersky Industrial CyberSecurity for Linux Nodes zu verwenden.

Wichtige Funktionen

Schutz vor massenhaften Cyberbedrohungen

Der Schutz auf Basis fortschrittlicher Technologien ist die Grundlage Ihrer IT-Sicherheit. Kaspersky Endpoint Security verhindert die Infektion der Dateisysteme von Benutzergeräten, überwacht den Anschluss von Wechseldatenträgern an das Gerät und untersucht diese auf Viren. Das Programm überwacht schädliche Aktivitäten von Programmen und schützt Dateien vor schädlicher Remote-Verschlüsselung. Datenbanken mit Informationen über neue globale Bedrohungen, wie Viren, Trojaner, Verschlüsselungstrojaner und Hackerangriffe, werden regelmäßig und automatisch aktualisiert.

Kommunikations- und Web-Schutz

Kaspersky Endpoint Security schützt die Netzwerkumgebung Ihres Unternehmens zuverlässig: Das Programm untersucht E-Mails, Websites und heruntergeladene Dateien auf Viren, Netzwerkwürmer und andere Bedrohungen, bevor Sie sie öffnen. Das Programm ermöglicht die Untersuchung des eingehenden Netzwerkverkehrs auf Aktivitäten, die auf einen Netzwerkangriff hinweisen können, überwacht die Einstellungen der Firewall des Betriebssystems und filtert die Netzwerkaktivität.

Sicherheitskontrollen am Arbeitsplatz

Durch die Verwendung von Kaspersky Endpoint Security zur Kontrolle des Benutzerzugriffs auf Programme, Webressourcen und verbundene Geräte am Arbeitsplatz stellen Sie eine weitere Sicherheitsebene für Ihr Unternehmen bereit. Dies hilft, Geräte vor Infektionen zu schützen und Datenverlust oder Datenlecks zu verhindern.

Schutz vor komplexen Bedrohungen und gezielten Angriffen

Das Programm kann mit Kaspersky-Lösungen für Detection and Response interagieren, nämlich mit Kaspersky Managed Detection and Response (MDR) und Kaspersky Anti Targeted Attack Platform (KATA). Die Kaspersky-SIEM-Lösung Kaspersky Unified Monitoring and Analysis Platform (KUMA) wird ebenfalls unterstützt. Kaspersky Endpoint Security überwacht die auf Benutzergeräten ausgeführten Prozesse, offenen Netzwerkverbindungen und geänderten Dateien. Die Interaktion mit Detection and Response-Lösungen bietet Schutz vor Bedrohungen wie Exploits, Ransomware, dateilosen Angriffen und legitimen Systemtools, mit denen Hacker Geräte oder Daten kompromittieren können.

Schutz von virtuellen und Cloud-Umgebungen

Kaspersky Endpoint Security als Teil der Lösung Kaspersky Security for Virtualization Light Agent bietet Schutz für virtuelle Maschinen, auf denen Linux-Gastbetriebssysteme auf verschiedenen Servervirtualisierungsplattformen und VDI-Plattformen ausgeführt werden. Die Untersuchung von Objekten auf Viren wird von einer speziellen Komponente durchgeführt, die auf einer separaten virtuellen Maschine, der SVM (Secure Virtual Machine), installiert ist. Auf diese Weise gewährleistet das Programm die Sicherheit, indem es die Ressourcen der SVM anstelle der Ressourcen der virtuellen Maschine verwendet. Dies minimiert zusammen mit der intelligenten Optimierung (z. B. der Verwendung eines gemeinsamen Caches) die Gesamtbelastung der IT-Infrastruktur.

Neuerungen in Version 12.5

Kaspersky Endpoint Security 12.5 für Linux bietet die folgenden neuen Funktionen und Verbesserungen:

- Unterstützung für die Installation von Kaspersky Endpoint Security 12.5 für Linux auf Geräten mit Elbrus-CPUs. Die Anwendung bietet eingeschränkte Unterstützung für Elbrus-CPUs.

- Die Integration mit Kaspersky Endpoint Detection and Response Expert (cloud) wurde implementiert. Diese Cloud-Lösung dient dazu, die IT-Infrastruktur der Organisation vor komplexen Cyberbedrohungen zu schützen, einschließlich solcher, die von EPP-Anwendungen, die auf Unternehmensressourcen installiert sind, nicht erkannt werden können. Die Lösung bietet umfassende Transparenz, Korrelation und Automatisierung durch die Nutzung einer breiten Palette von Reaktionstools und Datenquellen, einschließlich Endpoint-Assets, Netzwerkdaten und Daten aus Cloud-Umgebungen. Dadurch wird über integrierte Komponenten und End-to-End-Workflows innerhalb einer einzigen Oberfläche ein einheitlicher Detection-and-Response-Prozess ermöglicht, um die Effizienz von Sicherheitsspezialisten zu steigern.

  > Die Integration von Kaspersky Endpoint Security für Linux mit der Lösung Kaspersky Endpoint Detection and Response Expert (cloud) ist vorübergehend nicht verfügbar, bis diese Lösung eingeführt wird; dies ist für Ende 2026 geplant. Danach wird die Integration für diese Version von Kaspersky Endpoint Security voraussichtlich ohne zusätzliche Upgrades verfügbar sein.

- Kennwortschutz für bestimmte Aktionen im Programm Kaspersky Endpoint Security. Kennwortschutz ermöglicht es Ihnen, die Aktionen einzuschränken, die Benutzer entsprechend den ihnen gewährten Berechtigungen im Programm Kaspersky Endpoint Security ausführen können. Durch die Beschränkung des Zugriffs auf die Programmeinstellungen wird das Risiko unbefugter oder unbeabsichtigter Änderungen am Programm verringert.

- Die Komponente Gerätekontrolle wurde erweitert. Sie können jetzt die Liste der vertrauenswürdigen Geräte in eine Datei exportieren und aus einer Datei importieren.

- Verbesserte Komponente Schutz vor BadUSB-Angriffen. Wenn Sie jetzt einen Barcodescanner anschließen, können Sie einen Barcode vom Bildschirm scannen, um den Scanner zu autorisieren, anstatt einen Autorisierungscode zum Entsperren des Geräts einzugeben.

- Verbesserungen am aktualisierbaren Kernel-Modul (ULKM):
  - Die Unterstützung für das auf dem aktualisierbaren Kernel-Modul (ULKM) basierende Abfangen von Systemereignissen wurde für Systeme mit aktiviertem Secure Boot hinzugefügt.
  - Das Programm unterstützt jetzt mehr Betriebssysteme, auf denen das aktualisierbare Kernel-Modul zum Abfangen von Ereignissen verwendet werden kann.
  - Wir haben Unterstützung für das aktualisierbare Kernel-Modul für die Komponenten Schutz vor Verschlüsselung und Gerätekontrolle hinzugefügt.
- Wir haben den Installationsprozess im Modus der geschlossenen Softwareumgebung von Astra Linux Special Edition verbessert. Wenn jetzt ein Kompatibilitätspaket installiert ist, muss der Benutzer nach der Installation auf einem Gerät mit dem Betriebssystem Astra Linux Special Edition keine zusätzlichen Aktionen manuell ausführen, um das Programm Kaspersky Endpoint Security zu starten.
- Bei der Installation der Anwendung können Sie jetzt die Einstellungen der Konfigurationsdatei kesl.ini mithilfe der Konfigurationsdatei autoinstall.ini ändern.
- Verbesserte Fehlerdiagnose während der Installation und Deinstallation des Programms:
  - Rückgabecodes sind jetzt detaillierter, damit mögliche Probleme leichter verständlich sind.
  - Wir haben neue Meldungen zu fehlenden Abhängigkeiten (externe Bibliotheken, Komponenten, Dienstprogramme oder andere Programme) hinzugefügt, die für die Installation und den ordnungsgemäßen Betrieb des Programms erforderlich sind.
  - Wir haben neue Meldungen zu falsch konfigurierten Zugriffsberechtigungen für Systemverzeichnisse hinzugefügt.
  - Kaspersky Security Center zeigt neue und präzisierte Fehlermeldungen an.
  - Jetzt können Sie Fehler des Paketmanagers während der Installation des Programms ignorieren.
- Ein automatischer Programmneustart wurde für den Fall implementiert, dass innerhalb von 24 Stunden nach der Installation des Programms beim ersten Update der Datenbanken und Module kritische Updates empfangen werden.
- Jetzt können Sie das Programm so konfigurieren, dass es beim Erhalt kritischer Updates automatisch neu gestartet wird. Sie können den automatischen Neustart des Programms in den Richtlinieneigenschaften über die Web Console oder die Verwaltungskonsole oder über die Befehlszeile in den allgemeinen Programmeinstellungen konfigurieren.
- Bei der Integration mit Detection and Response-Lösungen können Sie den Ereigniscache jetzt mithilfe der Einstellung `UseIncreasedXdrEventsCache` in der Konfigurationsdatei kesl.ini verwalten. Es besteht ein Zielkonflikt zwischen hoher Leistung und RAM-Speicherbedarf.
- Sie können jetzt beim Beenden oder Neustarten des Programms mithilfe der Einstellung `FastShutdown` in der Konfigurationsdatei kesl.ini ein schnelles Beenden des Prozesses kesl ausführen, wodurch die Ausfallzeiten des Programms auf Systemen mit hoher Auslastung minimiert und ein übermäßiger Ressourcenverbrauch verhindert werden.
- Sie können jetzt den Speicherverbrauch der Komponente „Verhaltensanalyse“ für die Verarbeitung der Ereigniswarteschlange mithilfe der Einstellung `ReduceSWMemoryConsumption` aus der Konfigurationsdatei kesl.ini begrenzen. Die Verwendung dieser Einstellung kann sich auf das Schutzniveau auswirken. Lesen Sie unbedingt die Dokumentation.

- Wir haben die Stabilität des Netzwerkzugriffs verbessert. Wenn der kesl-Prozess jetzt nicht ordnungsgemäß beendet wird, entfernt der Watchdog-Server die Firewall-Regeln, die die Anwendung beim Start der Komponenten „Schutz vor Web-Bedrohungen“ und „Schutz vor Netzwerkbedrohungen“ hinzufügt. So können Sie vermeiden, dass die Internetverbindung verloren geht, und den Netzwerkzugriff auf dem Gerät schnell wiederherstellen.

- Sie können jetzt verhindern, dass mehrere Untersuchungsaufgaben gleichzeitig ausgeführt werden, um die Leistung der Anwendung zu optimieren. Wenn diese Option aktiviert ist, werden mehrere Untersuchungsaufgaben in eine Warteschlange gestellt, wenn sie gleichzeitig gestartet werden.

- Ausnahmen für Schutz vor bedrohlichen Dateien können jetzt symbolische Links verarbeiten. Pfade werden jetzt in endgültige Dateiadressen umgewandelt.

- Sie können das Verzeichnis für Dump-Dateien jetzt mithilfe des Befehls zur Verwaltung allgemeiner Anwendungseinstellungen aktivieren und konfigurieren, ohne die Anwendung neu zu starten. Diese Konfigurationseinstellungen für Dump-Dateien wurden aus der Konfigurationsdatei kesl.ini entfernt.

- Bei der Integration mit den Lösungen Kaspersky Endpoint Detection and Response Expert (on-premise), Kaspersky Anti Targeted Attack Platform und Kaspersky Unified Monitoring and Analysis Platform ist jetzt ein Kennwort erforderlich. Bei der Konfiguration der Integration müssen Sie jetzt ein Kennwort für das Client-Zertifikat angeben.

- Das Programm kann jetzt den Datenverkehr beim Senden von Telemetrieereignissen im Rahmen der Integration mit Kaspersky Unified Monitoring and Analysis Platform komprimieren, wodurch Bandbreite eingespart wird.

- Wir haben die Liste der unterstützten Betriebssysteme aktualisiert, einschließlich der Unterstützung für 64-Bit-Versionen von CentOS 5.2, 5.4, 6.4 und 6.6.

- Die Programmoberfläche ist in neuen Sprachen verfügbar: Spanisch (Mexiko) und Portugiesisch (Brasilien).

Änderungen in älteren Versionen

Version 12.4

Kaspersky Embedded Systems Security 12.4 für Linux bietet jetzt die folgenden neuen Funktionen und Verbesserungen:

- Die neue Funktionskomponente Schutz vor E-Mail-Bedrohungen wurde hinzugefügt. Die Komponente untersucht ein- und ausgehende E-Mail-Anhänge auf Viren und andere Bedrohungen.

- Die neue Funktionskomponente Schutz vor BadUSB-Angriffen wurde hinzugefügt. Diese Komponente verhindert, dass infizierte USB-Geräte, die sich als Tastaturen ausgeben, eine Verbindung mit dem Client-Gerät herstellen.

- Die Komponente Gerätekontrolle wurde erweitert. Bei Anfrage eines Benutzers kann diesem jetzt temporärer Zugriff auf gesperrte Geräte gewährt werden.

- Die Komponente Exploit-Prävention wurde weiter verbessert. Sie können jetzt komponentenspezifische Untersuchungsausnahmen für Objekte konfigurieren.

- Das aktualisierbare Kernel-Modul wurde weiter verbessert:

  - Das aktualisierbare Kernel-Modul ermöglicht jetzt die Optimierung des Abfangens von Dateioperationen. Die Anwendungsleistung wird durch die Verwendung eines Caches für Dateien und Prozesse, die keiner Überprüfung bedürfen, gesteigert.

  - Bei Verwendung des aktualisierbaren Kernel-Moduls können Sie globale Ausnahmen jetzt noch präziser anpassen. Wenn Sie den auf der fanotify-Technologie basierenden Abfangmechanismus verwenden, werden die angegebenen Mountpunkte vollständig vom Abfangen von Dateioperationen ausgeschlossen. Das aktualisierbare Kernel-Modul erlaubt das Ausschließen bestimmter, auf dem Gerät gemounteter lokaler Verzeichnisse oder Netzwerkverzeichnisse.

- Die Komponente EDR (KATA), die die Integration mit Kaspersky Endpoint Detection and Response (KATA) bereitstellt, wurde in EDR Expert (on-premise) umbenannt. Diese Komponente stellt außerdem die Integration in Kaspersky Endpoint Detection and Response Expert (on-premise) bereit. Die Integrationsaufgabe wurde in *Integration in Kaspersky Endpoint Detection and Response Expert (on-premise)* (KATAEDR, ID: 24) umbenannt.

- Sie können jetzt die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) einrichten. Diese Cybersecurity-Lösung für Unternehmen ermöglicht den Schutz vor den meisten Cybersecurity-Risiken und deckt die wichtigsten Szenarien der Verbreitung von Bedrohungen ab. Die Komponenten von Kaspersky Endpoint Detection and Response Expert (on-premise) werden auf der Open Single Management Platform (OSMP) bereitgestellt. Die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premises) unterstützt alle Möglichkeiten der Integration mit Kaspersky Endpoint Detection and Response (KATA) sowie neue Funktionen:

  - Starten einer YARA-Untersuchung. Bei einer *YARA-Untersuchung* verwendet Kaspersky Endpoint Security sogenannte YARA-Dateien, um auf einem Gerät nach Signaturen schädlicher Aktivitäten zu suchen.

  - Sammlung forensischer Daten. Dies sind digitale Daten, die bei Untersuchungen von Datenlecks und Vorfällen mit Bezug auf Cyberkriminalität nützlich sein können.

  - Senden erweiterter Daten über Ereignisse auf Geräten (Telemetriedaten) an die Telemetrieserver auf Basis der OSMP.

  - Senden ausschließlich von Telemetriedaten mit einem Angriffsindikator (Indicator of Attack, IOA). Sie können jetzt auch benutzerdefinierte Filter in der Web Console-Richtlinie konfigurieren.

  - Aktivierung der Komponente EDR Expert (on-premise), die die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) sowie die Integration mit Kaspersky Endpoint Detection and Response (KATA) bereitstellt, durch Hinzufügen eines Lizenzschlüssels.

  - Auswählen eines Integrationsmodus in den Einstellungen der Aufgabe *Integration in Kaspersky Endpoint Detection and Response Expert (on-premise)* über die Befehlszeile oder in den Richtlinieneigenschaften in der Web Console.

- Die Anwendung kann jetzt im Modus als Endpoint Detection and Response Agent verwendet werden, in dem sie auf geschützten Maschinen die gemeinsame Verwendung der Detection and Response-Lösungen von Kaspersky und der Anti-Virus-Anwendungen von Drittherstellern ermöglicht. In diesem Modus werden weder die standardmäßigen Schutzkomponenten noch die Kontrollkomponenten von Kaspersky Endpoint Security zum Schutz von Geräten verwendet. Der Standardschutz des Geräts wird durch die Anwendung eines Drittherstellers gewährleistet.

- Beim ersten Start der Anwendung nach ihrer Installation kann jetzt eine Protokolldatei für die Anwendung erstellt werden. Für den ersten Start der Anwendung in der Web Console, in der Verwaltungskonsole oder in den Parametern der Datei zur Erstkonfiguration können Sie jetzt die Erstellung von Protokolldateien aktivieren.

- In der Web Console wurde die Oberfläche für Richtlinien aktualisiert. Die Struktur der Abschnitte in der Richtlinie wurde überarbeitet, damit Sie die benötigten Funktionen schneller finden können.
- Sie können jetzt den Modus zum Abfangen des Datenverkehrs auswählen: die eBPF-Technologie oder das Tool iptables.
- Es ist jetzt möglich, die Quelle der Telemetriedaten auszuwählen (nur eBPF oder eBPF mit auditd). Für auditd können Sie auch die Arbeitsweise festlegen (exklusiver Modus oder Multicast-Modus).
- Sie können jetzt den Modus auswählen, in dem Dateien und Verzeichnisse zur Untersuchung an die Sandbox gesendet werden: manuell, nur automatisch, automatisch und manuell.
- Erweiterte Möglichkeiten der Anwendung bei Verwendung im Light Agent-Modus:
  - Es ist ein Mechanismus zum Abfangen von Systemereignissen auf Basis des aktualisierbaren Kernel-Moduls verfügbar.
  - Die funktionale Komponente Exploit-Prävention ist verfügbar.
  - Die Erkennung von Bedrohungen wurde weiter verbessert.
- Jetzt können Sie das Kaspersky Private Security Network (KPSN) direkt verwenden, ohne den KSN Proxy-Service auf dem Administrationsserver zu verwenden.
- Jetzt können Sie Richtlinien für mobile Benutzer in der Web Console und in der Verwaltungskonsole erstellen. Die Richtlinien für mobile Benutzer werden angewendet, wenn sich ein Gerät außerhalb des Netzwerks der Organisation befindet.
- Beim Anzeigen und Exportieren der Liste der Mountpunkte in der Web Console oder der Verwaltungskonsole sowie beim Anzeigen dieser Liste über die Befehlszeile werden jetzt auch Informationen zu einem in einem Namensraum gefundenen Mountpunkt angezeigt.
- Wir haben den alternativen Mechanismus zum Abrufen von Systemtelemetrie in der Komponente „Verhaltensanalyse“ auf 64-Bit-Betriebssystemen mit Kernel-Version 4.18 oder höher und eBPF-Unterstützung verbessert, sodass die Ressourcen des Kernel-Audit-Subsystems auditd freigegeben werden können.
- Bei einer Integration mit Kaspersky Managed Detection and Response wurde die Möglichkeit hinzugefügt, folgende Informationen in die Telemetriedaten aufzunehmen:
  - Indikator dafür, dass das Ereignis in einem Container aufgetreten ist
  - ID des Namensraums des Containers
  - Name des Containers
- Wir haben die Liste der unterstützten Betriebssysteme aktualisiert.

Version 12.3

Kaspersky Embedded Systems Security 12.3 für Linux bietet jetzt die folgenden neuen Funktionen und Verbesserungen:

- Es wurde ein Mechanismus zum Abfangen von Systemereignissen auf Basis des aktualisierbaren Kernel-Moduls hinzugefügt (nicht verfügbar im Light Agent-Modus). Wenn das Betriebssystem auf Ihrem Gerät die fanotify-Technologie unterstützt und zusätzlich die Anforderungen an die Installation des aktualisierbaren Kernel-Moduls erfüllt, können Sie die Verwendung des aktualisierbaren Kernel-Moduls zur Ausführung der Anwendung konfigurieren. Die Verwendung des aktualisierbaren Kernel-Moduls ermöglicht es, das Abfangen gestarteter Prozesse durch Kaspersky Endpoint Security zu optimieren. Das aktualisierbare Kernel-Modul ist im Lieferumfang der Anwendung enthalten.

- Das aktualisierbare Kernel-Modul verbessert die Funktionalität der Komponente Schutz vor Verschlüsselung (nicht verfügbar im Light Agent-Modus). Die Anwendung kann jetzt noch mehr Arten von Ransomware erkennen.

- Es wurde eine neue Funktionskomponente hinzugefügt: Exploit-Prävention (nicht verfügbar im Light Agent-Modus). Die Komponente überwacht Softwarecode, der Schwachstellen auf dem Gerät nutzt, um mittels Exploits Administratorrechte zu erlangen oder schädliche Aktionen auszuführen.

- Die Komponente Gerätekontrolle wurde erweitert:

  - Wir haben die Möglichkeit hinzugefügt, eine Liste von Benutzern oder Benutzergruppen zu konfigurieren, für die hinzugefügte Geräte als vertrauenswürdig gelten.

  - Es wurde die Möglichkeit hinzugefügt, nur lesenden Zugriff auf Geräte zum Speichern von Daten zu gewähren.

  - Außerdem haben wir die Benachrichtigung der Benutzer über Ereignisse verbessert, indem wir neue Ereignisse hinzugefügt sowie Ereignistexte in Plug-ins und in der Befehlszeile präzisiert und systematisiert haben.

- Erweiterte Möglichkeiten zur Integration mit der Lösung Kaspersky Managed Detection and Response:

  - Die Möglichkeit, Geräte vom Netzwerk zu isolieren, wurde implementiert.

  - Die Möglichkeit, Dateien in die Quarantäne zu verschieben und aus der Quarantäne wiederherzustellen, wurde implementiert.

  - Die Möglichkeit zum Starten von Prozessen und Beenden von Prozessen wurde implementiert.

- Wir haben die Möglichkeit hinzugefügt, die MDR-Komponente, welche die Integration mit Kaspersky Managed Detection and Response gewährleistet, durch das Hinzufügen eines Lizenzschlüssels zu aktivieren.

- Die Komponente Verhaltensanalyse wurde verbessert. Es wurde die Möglichkeit hinzugefügt, einen Prozess von der Untersuchung auszuschließen, wenn die Komponenten MDR und EDR (KATA) ausgeführt werden.

- Es wurde die Möglichkeit implementiert, Ausnahmen bei Verwendung eines Proxyservers zu konfigurieren. Sie können Anwendungskomponenten von Kaspersky Endpoint Security angeben, für deren Ausführung kein Proxyserver verwendet werden soll. Weiterhin können Sie Listen mit Adressen anlegen, für deren Verbindung kein Proxyserver verwendet werden soll. Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, wird die Verwendung eines Proxyservers für die Verbindung mit Kaspersky Security Network, zur SVM und zum Integrationsserver nicht unterstützt.

- Sie können jetzt Ausnahmen beim Abfangen des Datenverkehrs konfigurieren. Sie können jetzt die Verwaltungs-Plug-ins des Programms oder die Befehlszeile verwenden, um Verbindungen anzugeben, die vom Abfangen des Datenverkehrs durch das Programm ausgeschlossen werden sollen.

- Es wurde die Möglichkeit hinzugefügt, Dateien von Datenbankprotokollen temporär von der Untersuchung auszuschließen, um deren Untersuchung durch den Schutz vor bedrohlichen Dateien zu optimieren. Wenn eine Datenbankprotokolldatei innerhalb von 10 Minuten nach der letzten Untersuchung vom selben Prozess erneut verwendet wird, untersucht die Anwendung diese Protokolldatei nicht.

- Wenn die Einstellungen einer übergeordneten Richtlinie vererbt werden, können jetzt die Elemente aus den Ausnahmelisten der übergeordneten und untergeordneten Richtlinie vereinigt werden.

- Sie können jetzt das Verwaltungs-Web-Plug-in verwenden, um Ausnahmelisten in Richtlinien und Aufgaben zu exportieren und zu importieren.

- Es wurde die Möglichkeit hinzugefügt, die Parameter zur Erstkonfiguration von Kaspersky Endpoint Security wie folgt anzugeben: in der Kaspersky Security Center Verwaltungskonsole beim Erstellen des Installationspakets oder in den Eigenschaften des Installationspakets.

- Geplante Aufgaben können jetzt so konfiguriert werden, dass sie nicht auf Geräten ausgeführt werden, die sich im Batteriebetrieb befinden.

- Es wurde die Möglichkeit hinzugefügt, die Verwendung des KSN-Proxyservers bei der Kommunikation von Kaspersky Endpoint Security mit den KSN-Servern zu aktivieren und zu deaktivieren (im Light Agent-Modus nicht verfügbar). Wenn die Verwendung des KSN-Proxyservers aktiviert ist, interagiert Kaspersky Endpoint Security über den KSN Proxy-Service des Administrationsservers mit den KSN-Servern. Wenn die Verwendung des KSN-Proxyservers deaktiviert ist, kommuniziert Kaspersky Endpoint Security direkt mit den KSN-Servern.

- In der Befehlszeile können Sie einen Befehl verwenden, der eine Liste der Programmfunktionen, Informationen über deren Status (verwendet oder nicht verwendet) sowie die Linux-Technologien anzeigt, mit denen diese Funktionen des Programms implementiert sind.

- Es wurde die Möglichkeit hinzugefügt, Informationen über die auf dem Gerät geltende Richtlinie und die geltenden Richtlinienprofile in der Befehlszeile und in der grafischen Benutzeroberfläche anzuzeigen.

- Es wurde die Möglichkeit implementiert, die Anwendung mithilfe der Befehlszeile auf einem Gerät zu installieren, das keinen Perl-Interpreter besitzt.

- Wir haben das Abfangen des Datenverkehrs verbessert. Lokaler Datenverkehr (Datenverkehr zwischen Prozessen, die sich auf demselben Gerät befinden) wird jetzt nicht abgefangen.

- Es wurde die Möglichkeit implementiert, erforderliche Parameter zum Senden von Telemetriedaten bei einer Integration mit Kaspersky Managed Detection and Response zu übertragen, ohne die KPSN-Konfigurationsdatei zu verwenden. Wenn Sie die Infrastrukturlösung Kaspersky Security Network verwenden oder nur einen Root-Mandanten betreiben, ist für die Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response keine KPSN-Konfigurationsdatei erforderlich.

- Die Speicherung einer großen Anzahl von Ereignissen im Ereignisprotokoll der Anwendung wurde optimiert. Das Öffnen und Schließen der Ereignisdatenbank sowie das Abrufen von Ereignissen erfolgen jetzt schneller.

- Wir haben die grafische Benutzeroberfläche des Programms verbessert (wenn das Programm im Light Agent-Modus verwendet wird, wird die grafische Benutzeroberfläche nicht unterstützt):

  - Jetzt können Sie die Komponente Web-Kontrolle aktivieren oder deaktivieren.

  - Wir haben den Stil der grafischen Benutzeroberfläche überarbeitet (neue Farben, abgerundete Ecken aller Fenster).

- In den Einstellungen des Schutzes vor bedrohlichen Dateien und der Untersuchungsaufgaben wurden die Namen der Aktionen geändert, die auf infizierte Objekte angewendet werden.

- Für die Verhaltensanalyse wurde der alternative Mechanismus zum Abrufen der Systemtelemetrie auf 64-Bit-Betriebssystemen hinzugefügt (ab Kernel-Version 5.3 mit Unterstützung von eBPF). Dieser erlaubt das Freigeben von Ressourcen des Kernel-Audit-Subsystems auditd. Wenn das Betriebssystem die Anforderungen erfüllt, verwendet das Programm eBPF auch im Light Agent-Modus automatisch.

- Datum und Uhrzeit werden in allen Verwaltungsoberflächen des Programms (mit Ausnahme der Befehlszeilenschnittstelle) in einem einheitlichen Format gemäß RFC 3339 angezeigt, z. B. 2023-12-25 23:55:59.

- Wir haben die Liste der unterstützten Betriebssysteme aktualisiert.

Version 12.2

Kaspersky Embedded Systems Security 12.2 für Linux bietet jetzt die folgenden neuen Funktionen und Verbesserungen:

- Implementierung der Integration mit Kaspersky Network Detection and Response (KATA). Dies ist eine Komponente der Lösung "Kaspersky Anti Targeted Attack Platform", welche den Schutz für interne Unternehmensnetzwerke sicherstellt. Darüber hinaus können damit Informationen zu Ereignissen auf den Geräten (Telemetriedaten) an die Server von Kaspersky Anti Targeted Attack Platform mit der Komponente "Central Node" (siehe NDR-Server) übertragen werden.

- Implementierung der Integration mit KATA Sandbox. Dies ist eine Komponente der Lösung "Kaspersky Anti Targeted Attack Platform", welche die Ausführung und Analyse von verdächtigen Objekten erlaubt, um bösartige Aktivitäten und Anzeichen gezielter Angriffe auf die IT-Infrastruktur einer Organisation zu identifizieren. Für die Ausführung der Objekte werden spezielle Server verwendet, deren Betriebssysteme aus virtuellen Images installierten werden.

- Implementierung der Integration mit Kaspersky Unified Monitoring and Analysis Platform. Dies ist eine komplexe Software-Lösung, welche die folgenden Funktionalen Möglichkeiten vereint: Abrufen, verarbeiten und Speichern von Ereignissen mit Bezug auf die Informationssicherheit, Analyse und Korrelation eingehender Daten, Suche nach abgerufenen Ereignissen und Erstellung von Benachrichtigungen über identifizierte Anzeichen von Bedrohungen für die Informationssicherheit.

- Erweiterung der Integration mit Kaspersky Endpoint Detection and Response (KATA). Dies ist eine Komponente der Lösung Kaspersky Anti Targeted Attack Platform, mit folgenden erweiterten Funktionen:

  - Die Möglichkeit, das Starten eines Objekts zu verbieten, wurde implementiert.

  - Die Möglichkeit, Dateien in die Quarantäne zu verschieben, wurde implementiert.

  - Die Informationen zu Ereignissen auf Geräten (Telemetriedaten) wurden erweitert.

- Erweiterung der Integration mit Kaspersky Endpoint Detection and Response Optimum:

  - Die Möglichkeit, das Starten eines Objekts zu verbieten, wurde implementiert.

  - Die Möglichkeit, Dateien in die Quarantäne zu verschieben, wurde implementiert.

  - Die Möglichkeit, einen Prozess anhand seines Namens von der Netzwerkisolation auszuschließen, wurde implementiert.

- Es wurde die Möglichkeit zur Verwendung der Cloud Sandbox-Technologie hinzugefügt, mit der auf einem Gerät komplexe Bedrohungen erkannt werden können. Die Anwendung Kaspersky Endpoint Security sendet erkannte Dateien automatisch zur Analyse an Cloud Sandbox. Cloud Sandbox führt diese Dateien in einer isolierten Umgebung aus, um bösartige Aktivitäten zu erkennen und Entscheidungen über die Reputation dieser Dateien zu treffen.

- Es wurde die Möglichkeit implementiert, folgende Informationen anzuzeigen: Statistiken über die am häufigsten untersuchten Dateien und Anwendungen sowie eine Liste der auf dem geschützten Gerät erkannten Mountpunkte. Um die Leistung zu verbessern, können Sie jetzt den Untersuchungsausschlüssen folgende Objekte hinzufügen: Dateien, die am häufigsten von der Komponente "Schutz vor bedrohlichen Dateien" untersucht werden, Pfade der Anwendungen, die von der Komponente "Verhaltensanalyse" am häufigsten untersucht werden, Mountpunkte, die auf dem Gerät erkannt wurden.

- Jetzt können Sie Metriken zur Performance des Programms sammeln, mit denen die Auswirkungen von Kaspersky Endpoint Security auf die Leistung des Betriebssystems analysiert werden können.

- Die Komponente Firewall-Verwaltung wurde überarbeitet. Es können jetzt mehrere IP-Adressen oder IP-Adressbereiche für eine Netzwerkpaketregel angegeben werden.

- Es wurde ein Mechanismus zur Überwachung von Abstürzen des Betriebssystems hinzugefügt. Der Mechanismus überprüft bestimmte Systemfunktionen wie execve auf Abstürze. Der wdserver-Prozess des Watchdog-Servers startet alle drei Sekunden einen weiteren wdserver-Prozess, in welchem diese Systemfunktionen aufgerufen werden (der Aufruf der Funktion execve startet mindestens noch einen weiteren wdserver-Prozess). Wenn wdserver eine nicht reagierende Systemfunktion erkennt, startet der Watchdog-Server den kesl-Prozess neu.

- Das Anzeigen von Popup-Benachrichtigungen konfiguriert werden, wenn die grafische Benutzeroberfläche der Anwendung verwendet wird. Jetzt können Sie die Anzeige von Popup-Benachrichtigungen in der grafischen Benutzeroberfläche über die Web Console, die Verwaltungskonsole oder die Befehlszeile aktivieren oder deaktivieren.

- Die Parameter für den Aufgabenzeitplan in der Befehlszeile wurden überarbeitet. Sie können eine Aufgabe jetzt so konfigurieren, dass sie bei Erreichen der maximal zulässigen Ausführungszeit automatisch gestoppt wird.

- Beim Erstellen eines Richtlinienprofils von Kaspersky Security Center wurde der Status der mit einem Schloss versehenen Attribute geändert. Beim Erstellen eines Standardprofils sind jetzt alle Schlösser entsperrt, sodass die Profileinstellungen standardmäßig nicht die Basis-Einstellungen einer Richtlinie überschreiben.

- Es wurde ein alternativer Mechanismus zum Abrufen der Systemtelemetrie auf 64-Bit-Betriebssystemen hinzugefügt (ab Kernel-Version 5.3 mit Unterstützung von eBPF mit BTF), der das Freigeben von Ressourcen des Kernel-Audit-Subsystems "auditd" erlaubt. Die Anwendung arbeitet automatisch mit eBPF, wenn das Betriebssystem die angegebenen Voraussetzungen erfüllt.

- Die Anzeige von Datum und Uhrzeit wurde für allen Verwaltungs-Plug-ins der Anwendung auf das RFC 3339-Format angeglichen, z. B. 2023-12-25 23:55:59.

- Wir haben die Liste der unterstützten Betriebssysteme aktualisiert.

Version 12.1

Kaspersky Embedded Systems Security 12.1 für Linux bietet jetzt die folgenden neuen Funktionen und Verbesserungen:

- Sie können jetzt die Integration mit Kaspersky Endpoint Detection and Response Optimum einrichten. Diese Lösung schützt die IT-Infrastruktur des Unternehmens vor Bedrohungen wie Exploits, Ransomware, dateilosen Angriffen und der Verwendung legitimer Systemtools durch Angreifer zur Beschädigung von Geräten oder Daten.

- 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.

- Mit der *Web-Kontrolle* wurde eine neue funktionale Komponente hinzugefügt, die den Benutzerzugriff auf Webressourcen steuert. Dadurch können Sie den Datenverkehrsverbrauch senken und die unangemessene Nutzung der Arbeitszeit reduzieren. 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 des Programms können Sie jetzt die Einstellungen für die Erstkonfiguration angeben, die zuvor 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.

- Sie können jetzt Informationen über alle Geräte, die auf Client-Geräten installiert oder mit diesen verbunden sind (einschließlich Geräten, die zuvor installiert und verbunden waren, aber derzeit getrennt sind), an den Administrationsserver senden, wenn das Programm mit Kaspersky Security Center verwaltet wird.

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

- Wir haben die Liste der unterstützten Betriebssysteme aktualisiert.

Behobene Probleme

In der folgenden Tabelle sind alle Probleme aufgeführt, die in früheren Versionen von Kaspersky Endpoint Security gefunden und in der aktuellen Version behoben wurden.

Liste der in Version 12.5 behobenen Probleme

ID (Kennung)	Description
10306343	Beim Überprüfen des Status eines aktuellen Lizenzschlüssels wurden fälschlicherweise Benachrichtigungen über das Entfernen und Installieren eines Lizenzschlüssels generiert.
10295949	Die im aktuellen Richtlinienprofil für die Komponente Gerätekontrolle angegebenen Einstellungen wurden nicht übernommen. Infolgedessen arbeitete die Komponente weiterhin mit den in der Richtlinie festgelegten Einstellungen.
10171454	Wenn die erste in den Einstellungen angegebene Update-Quelle nicht verfügbar war, wurde fälschlicherweise eine Meldung über ein Update-Problem angezeigt.

ID (Kennung)	Description
10109293	Wenn der iptables-Modus zum Abfangen des Netzwerkdatenverkehrs ausgewählt war (`NetInterceptorMode=UseIPTables`), wurde der Datenverkehr von Programmen, die an eine bestimmte Netzwerkschnittstelle gebundene Netzwerk-Sockets öffnen, falsch verarbeitet.
10024219	Die Kaspersky Security Center Verwaltungskonsole zeigte den Status des aktualisierbaren Kernel-Moduls auf verwalteten Geräten falsch an.
9995631	Die Beschränkung der Nutzung des residenten Arbeitsspeichers durch das Programm (Einstellung `MaxMemory`) funktionierte auf Systemen ohne Swap-Partition nicht ordnungsgemäß. Wenn das festgelegte Limit erreicht wird, wird Kaspersky Endpoint Security jetzt neu gestartet.
9937329	Auf Systemen, auf denen die Aufgabe Gerätekontrolle (Device_Control) deaktiviert war, wurden *Gerät angeschlossen* und *Gerät getrennt* fälschlicherweise generiert.
9934846	Das Programm startete auf Systemen mit hoher Auslastung nicht. Die Zeitüberschreitung für die Verbindung des Programms mit dem Watchdog-Server wurde erhöht.
9846405	Auf Systemen mit konfiguriertem EFI-Bootloader wurden fälschlicherweise *Objekt nicht verarbeitet*-Ereignisse generiert.
9815051	Bereits hergestellte Netzwerkverbindungen konnten hängen bleiben, wenn die Aufgaben Schutz vor Web-Bedrohungen (Web_Threat_Protection) und Schutz vor Netzwerkbedrohungen (Network_Threat_Protection) auf verwalteten Geräten im eBPF-Modus zum Abfangen des Netzwerkdatenverkehrs (`NetInterceptorMode=UseEBPF`) ausgeführt wurden. Solche Verbindungen werden jetzt getrennt, wenn versucht wird, Daten zu übertragen.
9807202	Auf einigen ROSA-Betriebssystemen traten bei Verwendung des Dienstprogramms mkfs.ext2 Probleme bei der Installation auf.
9704644	Der Gerätestatus wurde falsch angezeigt, wenn das Programm im EDR-Agent-Modus verwendet wurde. Der Wert des Schutzstatus des Geräts bei Verwendung des Programms im EDR-Agent-Modus wurde geändert.
9643969	In einigen Fällen kann bei Verwendung des Abfangens von Netzwerkverkehr im eBPF-Modus ein Problem mit der Netzwerkkonnektivität zwischen Scylla-Hosts auftreten.
9633030	Die Aufgabe Ausführungsprävention für Objekte (EDR Expert (on-premises)) wurde ausgeführt, wenn das Kontrollkästchen **Ausführungsprävention für Objekte aktivieren** in der Richtlinie deaktiviert war.
9627894	Der auf der eBPF-Technologie basierende Modus zum Abfangen des Netzwerkdatenverkehrs funktionierte auf Betriebssystemen mit deaktiviertem IPv6 nicht ordnungsgemäß.
9606448	Beim Aktivieren des Programms mithilfe des Kaspersky Security Center Administrationsservers als Proxyserver für den Zugriff auf die Kaspersky-Aktivierungsserver trat ein Problem auf (wenn in der Richtlinie das Kontrollkästchen **Kaspersky Security Center als Proxyserver für die Aktivierung verwenden** aktiviert war).
9508605	Bei aktivierter Integration von Kaspersky Endpoint Detection and Response Expert belegte das Programm auf Systemen mit einer Container-Umgebung viel Arbeitsspeicher.
9456741	Das Programm stürzte ab, weil beim Abfangen des Starts eines neuen Prozesses der Dateiinterpreter nicht ermittelt werden konnte.

Liste der im Web-Plug-in 12.5.0.7391 behobenen Probleme

ID (Kennung)	Description
9558745	Die Einstellung **Pop-up-Benachrichtigungen auf der grafischen Benutzeroberfläche anzeigen** zur Konfiguration der Anzeige von Benachrichtigungen in der grafischen Benutzeroberfläche von Kaspersky Endpoint Security wurde in den Richtlinieneigenschaften (**Anwendungseinstellungen → Allgemeine Einstellungen → Ereigniseinstellungen → Erweiterte Einstellungen**) nicht angezeigt.
9622658	Beim Hinzufügen von Ausnahmen von der Schadsoftware-Untersuchung anhand des Objekt-Hashes wurden diese Ausnahmen nicht gespeichert.
9798821	Beim Hinzufügen einer einzelnen Website zu einer Web-Kontrolle-Regel wurden die Änderungen an der Richtlinie nicht gespeichert.
9990129	Im Formular zum Hinzufügen eines vertrauenswürdigen Programms wurde ein irrelevantes Feld **Kommentar** angezeigt.
9977884	In den Einstellungen der Komponente Schutz vor E-Mail-Bedrohungen wurde ein irrelevanter Umschalter **Sicherheitsstufe** angezeigt.
9944635	Der Name der Flags **E-Mail-Datenbanken untersuchen** wurde dupliziert. Jetzt werden die korrekten Namen angezeigt: **E-Mail-Datenbanken untersuchen** und **Dateien in E-Mail-Formaten untersuchen**.

ID (Kennung)	Description
10010439	Beim Erstellen von Regeln für die Web-Kontrolle wurde der Benutzer, der der Regel aus der Active Directory-Liste zugewiesen wurde, nicht ordnungsgemäß hinzugefügt.
10218308	Der Modus von Kaspersky Security Network wurde beim Ändern der Richtlinieneinstellungen zurückgesetzt.

Hard- und Softwarevoraussetzungen

Hardware-Mindestanforderungen

Für die Installation der Anwendung

- Ein Prozessor mit AMD64-Architektur, 2 GHz oder höher, mit mindestens zwei Kernen und Unterstützung für SSE2-Befehle.
- Swap-Speicher von mindestens 1 GB
- Arbeitsspeicher:
  - Für 64-Bit-Betriebssysteme: 2 GB RAM, das für die Anwendung verfügbar ist
  - Für 32-Bit-Betriebssysteme: 1 GB RAM, das für die Anwendung verfügbar ist
- 4 GB freier Speicher auf der Festplatte für die Installation der Anwendung und zur Speicherung von temporären Dateien und Protokolldateien

  Zum Speichern von Protokolldateien der Anwendung und Dump-Dateien der Anwendung ist auf dem Datenträger zusätzlicher Platz erforderlich.

  Beim Untersuchen von Archiven und zusammengesetzten Objekten mittels des Schutzes vor bedrohlichen Dateien und der Untersuchungsaufgaben wird außerdem zusätzlicher Speicherplatz benötigt. Die Menge dieses Speicherplatzes hängt von Typ und Größe dieser entpackten Objekte ab, wenn die Parameter `ScanArchived=Yes` und/oder `ScanSfxArchived=Yes` festgelegt sind (standardmäßig sind diese Parameter für Untersuchungsaufgaben auf `Yes` und für den Schutz vor bedrohlichen Dateien auf `No` festgelegt).

  Beim Untersuchen von Archiven und zusammengesetzten Objekten wird es empfohlen, ausreichend Platz im Verzeichnis "/tmp" bereitzustellen. Außerdem können Sie die Größe der zu untersuchenden Archive (im entpackten Zustand) anhand des Parameters `SizeLimit` für jede Aufgabe begrenzen.

Zur Installation der grafischen Benutzeroberfläche

- Ein Monitor, der Fenster mit einer Breite von 1000 Pixeln und einer Höhe von 600 Pixeln anzeigen kann. Wenn die Bildschirmskalierung angewendet wird, werden diese Abmessungen ebenfalls skaliert.

Minimale Hardwarevoraussetzungen für die Arm-Architektur

Für die Installation der Anwendung

- 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, welcher der Anwendung zur Verfügung steht.
- 3 GB freier Speicher auf der Festplatte für die Installation der Anwendung und zur Speicherung von temporären Dateien und Protokolldateien

  Zum Speichern von Protokolldateien der Anwendung und Dump-Dateien der Anwendung ist auf dem Datenträger zusätzlicher Platz erforderlich.

  Beim Untersuchen von Archiven und zusammengesetzten Objekten mittels des Schutzes vor bedrohlichen Dateien und der Untersuchungsaufgaben wird außerdem zusätzlicher Speicherplatz benötigt. Die Menge dieses Speicherplatzes hängt von Typ und Größe dieser entpackten Objekte ab, wenn die Parameter `ScanArchived=Yes` und/oder `ScanSfxArchived=Yes` festgelegt sind (standardmäßig sind diese Parameter für Untersuchungsaufgaben auf `Yes` und für den Schutz vor bedrohlichen Dateien auf `No` festgelegt).

  Beim Untersuchen von Archiven und zusammengesetzten Objekten wird es empfohlen, ausreichend Platz im Verzeichnis "/tmp" bereitzustellen. Außerdem können Sie die Größe der zu untersuchenden Archive (im entpackten Zustand) anhand des Parameters `SizeLimit` für jede Aufgabe begrenzen.

Zur Installation der grafischen Benutzeroberfläche

- Ein Monitor, der Fenster mit einer Breite von 1000 Pixeln und einer Höhe von 600 Pixeln anzeigen kann. Wenn die Bildschirmskalierung angewendet wird, werden diese Abmessungen ebenfalls skaliert.

Hardware-Mindestanforderungen für die Elbrus (E2K)-Architektur

Für die Installation der Anwendung

- CPU v3: Elbrus-4S; v4: Elbrus-8S oder Elbrus-1S+
- Mindestens 2 GB für die Swap-Partition.
- 2 GB RAM, welcher der Anwendung zur Verfügung steht.
- 2 GB freier Speicher auf der Festplatte für die Installation der Anwendung und zur Speicherung von temporären Dateien und Protokolldateien

Zur Installation der grafischen Benutzeroberfläche

- Ein Monitor, der Fenster mit einer Breite von 1000 Pixeln und einer Höhe von 600 Pixeln anzeigen kann. Wenn die Bildschirmskalierung angewendet wird, werden diese Abmessungen ebenfalls skaliert.

Softwarevoraussetzungen

Um Kaspersky Endpoint Security zu installieren, muss eines der in der Tabelle aufgeführten Betriebssysteme auf dem Gerät installiert sein:

In diesem Artikel werden die Softwareversionen aufgeführt, auf denen das Programm getestet wurde und für die eine ordnungsgemäße Funktion garantiert wird. Das Programm funktioniert möglicherweise auch mit anderen Softwareversionen, diese Konfigurationen wurden jedoch keinem vollständigen Testzyklus unterzogen und sind nicht in der Liste der garantiert unterstützten Versionen enthalten.

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

Der Schutz vor bedrohlichen Dateien für Mount-Punkte über die FUSE-Technologie ist ohne zusätzliche Schritte eingeschränkt, die der Administrator des Betriebssystems ausführen muss. Sie können die Einstellung user_allow_other zur Datei /etc/fuse.conf und die Mount-Option allow_root für jeden Mount-Punkt hinzufügen, damit die Anwendung Dateiereignisse an diesen Mount-Punkten überwachen kann.

64-Bit-Betriebssysteme	64-Bit-Betriebssysteme für die Arm-Architektur	64-Bit-Betriebssysteme für die Elbrus-(E2K)-Architektur	32-Bit-Betriebssysteme
• AlmaLinux OS 8.6, 8.7, 8.8, 8.9 • AlmaLinux OS 9.4, 9.5, 9.6 • AlterOS® 2025. • Amazon™ Linux 2023 • Astra Linux Common Edition Orel 2.12 • Astra Linux Special Edition RUSB.10015-01 (operational Update 1.5, 1.6, 1.7, 1.8). • Astra Linux Special Edition RUSB.10015-03 (reguläres Update 7.6) • Astra Linux Special Edition RUSB.10015-16 (Release 1) (operational Update 1.6) • Astra Linux Special Edition RUSB.10015-17 (operational Update 1.7.3) • Astra Linux Special Edition RUSB.10015-37 (reguläres Update 7.7) Das Betriebssystem Astra Linux im Modus "Mobile" wird nur im Desktop-Modus unterstützt. • CentOS 5.2, 5.4, 6.4, 6.6, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9. In der Lösung Kaspersky Endpoint Security Cloud wird die Ausführung der Anwendung auf Geräten mit CentOS 5.2, 5.4, 6.4, 6.6 nicht unterstützt. In Kaspersky Security Center Cloud Console wird die Ausführung der Anwendung auf Geräten mit CentOS 5.2, 5.4, 6.4, 6.6 nicht unterstützt. • CentOS Stream 8, 9, 10. • Debian GNU/Linux 12.8, 12.9, 12.10, 12.11, 12.12, 12.13. • Debian GNU/Linux 13.1, 13.2, 13.3 • EMIAS 1.0 • EulerOS 2.0 SP10 • Fedora Linux 41 • Kylin Desktop OS V10 SP1. • Linux Mint 21.3 • Linux Mint 22.2 • Mostech 12 Release 2021.1 • openSUSE Leap 15.6 • Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 • Oracle Linux 8.5, 8.6, 8.7, 8.8, 8.9 • Oracle Linux 9.4, 9.5, 9.6 • Red Hat Enterprise Linux 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 • Red Hat Enterprise Linux 8.5, 8.6, 8.7, 8.8, 8.9, 8.10. • Red Hat Enterprise Linux 9.4, 9.5, 9.6 • Red Hat Enterprise Linux 10.0, 10.1 • Rocky Linux 8.6, 8.7, 8.8, 8.9 • Rocky Linux 9.4, 9.5, 9.6 • SberLinux 8.10, 9.1, 9.5, 9.6, 9.7. • SberOS 3.4.0, 3.5.0, 3.6.1. • SUSE Linux Enterprise Server 12.5, 12.6, 12.7 • SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7 • Ubuntu® 24.04 LTS. • Ubuntu 26.04 LTS. • ALT Bildung 10, 11. • ALT Workstation 11 • ALT Server 11 • ALT SP Workstation Release 10 • ALT SP Server Release 10 • Atlant, Build Alcyone, Version 2022.02 • GosLinux 7.2. • M OS 12 Server Release 2021.1.	• Astra Linux Special Edition RUSB.10152-02 (reguläres Update 4.7) • CentOS Stream 9 • EulerOS 2.0 SP10 • SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7 • Ubuntu 26.04 LTS. • ALT Workstation 11.2 • ALT Server 11.1 • ALT SP Workstation Release 10 • ALT SP Server Release 10 • RED OS 8,0.	• OS Elbrus 9.3.6. • Astra Linux Special Edition RUSB.10015-16 (Release 2) (operational Update 8.1) • Astra Linux Special Edition RUSB.10265-01 (reguläres Update 8.1) • ALT SP Workstation Release 8, 10. • ALT SP Server Release 8, 10.	• Debian GNU/Linux 12.8, 12.9, 12.10, 12.11, 12.12, 12.13.

64-Bit-Betriebssysteme	64-Bit-Betriebssysteme für die Arm-Architektur	64-Bit-Betriebssysteme für die Elbrus-(E2K)-Architektur	32-Bit-Betriebssysteme
• Mos OS 15.5 Arbat • MSVSphere 9.5 ARM • MSVSphere 9.5 Server • OS MESH 12 für Moskauer Schulen – Version für interaktive Tafeln (mit Telemetrie und DIT-Unterstützung) Release 2025 • OS MESH 12 für Moskauer Schulen - Computer und Laptops (mit Telemetrie und DIT-Unterstützung) Release 2025 • OSnova 3.1. • RED OS® 7.3. • RED OS 8,0. • ROSA Cobalt 7.9 Workstation • ROSA Cobalt 7.9 Server • ROSA Chrome 12 Workstation • ROSA "Chrom" 12 Server • ROSA 13.1 • SintezM-Client 8.6 • SintezM-Server 8.6			

Zusätzliche Software- und Hardwareanforderungen für den Light Agent-Modus

Die Anwendung "Kaspersky Endpoint Security" kann in Form des Light Agent als Teil der Lösung Kaspersky Security for Virtualization Light Agent Version 6.5 verwendet werden. Sie können die Anforderungen an virtuelle Infrastrukturen für den Betrieb der Anwendung im Light Agent-Modus in der Hilfe zu Kaspersky Security for Virtualization Light Agent einsehen.

Virtuelle Maschinen

Für virtuelle Maschinen mit Kaspersky Endpoint Security im Light Agent-Modus gelten die Software- und Hardwareanforderungen von Kaspersky Endpoint Security mit den folgenden Einschränkungen:

- Eine virtualisierte Netzwerkschnittstelle mit einer Bandbreite von 100 Mbit/s ist erforderlich
- Auf Arm-Geräten wird Kaspersky Endpoint Security im Light Agent-Modus nicht unterstützt.
- Die Anwendung im Light Agent-Modus wird in den Betriebssystemen Astra Linux Special Edition im Modus der obligatorischen Zugriffskontrolle und im Modus der geschlossenen Softwareumgebung nicht unterstützt.

Das BIOS auf einer virtuellen Maschine muss die SMBIOS-Spezifikation Version 2.1 oder höher unterstützen.

Abhängig von Ihrer virtuellen Infrastruktur muss auf den virtuellen Maschinen Folgendes installiert sein:

- In einer Microsoft Hyper-V-Infrastruktur das Integration Services-Paket.
- In einer VMware vSphere-Infrastruktur das VMware Tools-Paket.
- In einer XenServer-Infrastruktur die XenTools-Software.
- In einer HUAWEI FusionSphere-Infrastruktur das HUAWEI Tools-Paket.
- In einer KVM-Infrastruktur (Kernel-based Virtual Machine) den QEMU Guest Agent.

Unterstützte Terminalserver-Typen

- Astra Linux 3.0.5-Terminalserver.

Lieferumfang

Der Lieferumfang von Kaspersky Endpoint Security umfasst die folgenden Dateien:

Hauptdateien des Programms

- Für Prozessoren mit 32-Bit-Betriebssystem:
  `kesl-12.5.0-<build number>.i386.rpm`
  `kesl_12.5.0-<build number>_i386.deb`
- Für Prozessoren mit 64-Bit-Betriebssystem:
  `kesl-12.5.0-<build number>.x86_64.rpm`
  `kesl_12.5.0-<build number>_amd64.deb`
- Für Arm®-Prozessoren, 64-Bit-Betriebssystem:
  `kesl-12.5.0-<build number>.aarch64.rpm`
  `kesl_12.5.0-<build number>_arm64.deb`
- Für Elbrus-CPU:
  `kesl-12.5.0-<build number>.e2k.rpm`
  `kesl_12.5.0-<build number>_e2k.deb`

Grafische Benutzeroberfläche des Programms

- Für Prozessoren mit 32-Bit-Betriebssystem:
  `kesl-gui-12.5.0-<build number>.i386.rpm`
  `kesl-gui_12.5.0-<build number>_i386.deb`
- Für Prozessoren mit 64-Bit-Betriebssystem:
  `kesl-gui-12.5.0-<build number>.x86_64.rpm`
  `kesl-gui_12.5.0-<build number>_amd64.deb`
- Für Arm®-Prozessoren, 64-Bit-Betriebssystem:
  `kesl-gui-12.5.0-<build number>.aarch64.rpm`
  `kesl-gui_12.5.0-<build number>_arm64.deb`
- Für Elbrus-CPU:
  `kesl-gui-12.5.0-<build number>.e2k.rpm`
  `kesl-gui_12.5.0-<build number>_e2k.deb`

Um das Programm Kaspersky Endpoint Security auf Betriebssystemen mit eingeschränkter Unterstützung (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6) zu installieren, wählen Sie das mit `OLD` gekennzeichnete Programmpaket aus.

Archiv für die Remote-Installation des Programms mithilfe von Kaspersky Security Center

`kesl-12.5.0.<build number>.zip`

Das Archiv enthält auch die Texte der Benutzervereinbarungen.

Texte der Benutzervereinbarungen

- `ksn_license.<language ID>` enthält den Text der Erklärung zu Kaspersky Security Network.
- `license.<language ID>` enthält den Text des Endbenutzer-Lizenzvertrags. Der Endbenutzer-Lizenzvertrag legt die Bedingungen für die Nutzung des Programms fest.

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

Kompatibilität mit anderen Programmen

Unterstützte Versionen von Kaspersky Security Center

Abhängig vom Modus von Kaspersky Endpoint Security können Sie das Programm mithilfe der in der Tabelle aufgeführten Versionen von Kaspersky Security Center verwalten.

Mode	Version von Kaspersky Security Center
Kaspersky Endpoint Security im Standard-Modus	Kaspersky Security Center Windows 14.2, 15.1. Verwaltung über die Verwaltungskonsole mithilfe des MMC-Verwaltungs-Plug-ins und über die Kaspersky Security Center Web Console mithilfe des Web-Verwaltungs-Plug-ins. Kaspersky Security Center Linux 15.1, 15.2, 15.3, 15.4, 16.0, 16.1, 16.2, 16.3. Verwaltung über die Kaspersky Security Center Web Console mithilfe des Web-Verwaltungs-Plug-ins.
Kaspersky Endpoint Security im Standard-Modus mit der Komponente Endpoint Detection and Response Optimum	Kaspersky Security Center Windows 15.1. Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2.
Kaspersky Endpoint Security im Light Agent-Modus	Kaspersky Security Center Windows 15.1. Kaspersky Security Center Linux 16.1, 16.2, 16.3.
Kaspersky Endpoint Security im EDR Agent-Modus	Kaspersky Security Center Windows 14.2, 15.1. Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2, 16.3.

Unterstützte Version von Kaspersky Security for Virtualization Light Agent

Die Anwendung "Kaspersky Endpoint Security" kann in Form des Light Agent als Teil der Lösung Kaspersky Security for Virtualization Light Agent Version 6.5 verwendet werden.

Unterstützte Versionen der Lösung auf den KATA- und OSMP-Plattformen

Kaspersky Endpoint Security ist mit Lösungen auf Basis der Kaspersky Anti Targeted Attack Platform und mit der Lösung Kaspersky Endpoint Detection and Response Expert (on-premise) in folgenden Versionen kompatibel:

- Kaspersky Anti Targeted Attack Platform 6.0, 6.1, 7.0, 7.1 (Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), einschließlich Szenarien zum Senden von Dateien an die Sandbox zur Untersuchung).
- Kaspersky Anti Targeted Attack Platform 8.0 (Kaspersky Network Detection and Response (KATA), einschließlich Szenarien zum Senden von Dateien an die Sandbox zur Untersuchung).

  Weitere Informationen über Kaspersky Anti Targeted Attack Platform finden Sie in der Hilfe zu Kaspersky Anti Targeted Attack Platform.
- Kaspersky Endpoint Detection and Response Expert (on-premises) 8.0, 8.1, 8.2 auf der Open Single Management Platform (im Folgenden auch als OSMP bezeichnet), einschließlich Szenarien zum Senden von Dateien an die Sandbox zur Untersuchung.

  Weitere Informationen zu Kaspersky Endpoint Detection and Response Expert (on-premise) finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premise).

Unterstützte Versionen des Administrationsagenten für die Integration mit Kaspersky Endpoint Detection and Response Expert (cloud)

Für die Integration des Programms mit Kaspersky Endpoint Detection and Response Expert (cloud) benötigen Sie einen Administrationsagenten für Kaspersky Security Center Cloud Console bestimmter Versionen, die in der Hilfe zu Kaspersky Security Center Cloud Console beschrieben sind.

Kompatibilität mit Drittanbieterlösungen

Kaspersky Endpoint Security im EDR Agent-Modus kann mit der Antiviren-Anwendung Dr. Web zusammenarbeiten.

Vergleich des Funktionsumfangs verschiedener Kaspersky-Lösungen

Kaspersky Endpoint Security ist in vielen plattformübergreifenden Kaspersky-Lösungen enthalten. Der verfügbare Funktionsumfang der App wird durch die Lösung bestimmt, die Sie bei einem Dienstanbieter in Ihrer Region erworben haben.

Funktion	Kaspersky Next EDR Foundations	Kaspersky Next EDR Optimum	Kaspersky Next XDR Optimum	Kaspersky Next MXDR Optimum	Kaspersky Next EDR Expert	Kaspersky Next XDR Expert	Kaspersky Hybrid Cloud Security, Desktop	Kaspersk Cloud S Enter Desktop/C
Komponente "Schutz vor bedrohlichen Dateien".	✓	✓	✓	✓	✓	✓	✓	✓
Schutz vor E-Mail-Bedrohungen	✓	✓	✓	✓	✓	✓	✓	✓
Schutz vor Web-Bedrohungen	✓	✓	✓	✓	✓	✓	✓	✓
Schutz vor Netzwerkbedrohungen	✓	✓	✓	✓	✓	✓	✓	✓
Firewall-Verwaltung	✓	✓	✓	✓	✓	✓	✓	✓
Verhaltensanalyse	✓	✓	✓	✓	✓	✓	✓	✓
Schutz vor modifizierten USB-Geräten	–	✓	✓	✓	✓	✓	✓	✓
Gerätekontrolle	✓	✓	✓	✓	✓	✓	✓	✓
Untersuchung von Wechseldatenträgern	✓	✓	✓	✓	✓	✓	✓	✓
Schutz vor Verschlüsselung (für freigegebene Ordner)	✓	✓	✓	–	✓	✓	–	✓
Container untersuchen	–	–	–	–	–	✓	–	✓
Programmkontrolle	✓	✓	✓	✓	✓	✓	✓	✓
Web-Kontrolle	✓	✓	✓	✓	✓	✓	✓	✓
Integration mit Kaspersky Unified Monitoring and Analysis Platform	–	–	–	–	–	✓	–	-
Integration mit Kaspersky Endpoint Detection and Response Expert (cloud)	–	–	–	–	✓	✓	–	-
Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise)	–	–	–	–	✓	✓	–	-
Kaspersky Endpoint Detection and Response Optimum	✓	✓	✓	✓	–	–	–	-
Integration von Kaspersky Managed Detection and Response	–	–	–	✓	–	–	–	-

Bereitstellung und Erstkonfiguration

Sie können dieses Szenario befolgen, um Kaspersky Endpoint Security bereitzustellen und für die Verwendung vorzubereiten.

1 Nutzungsmodus auswählen

Nachdem Sie eine Kaspersky-Lösung auf der offiziellen Kaspersky-Website oder bei einem unserer Partner erworben haben, erhalten Sie eine Nachricht an die E-Mail-Adresse, die Sie beim Kauf angegeben haben. Diese Nachricht enthält einen Aktivierungscode und Informationen darüber, wie Sie eine Schlüsseldatei erhalten. Sie benötigen möglicherweise eine Schlüsseldatei, wenn Ihr Unternehmen die Online-Aktivierung des Programms mithilfe eines Codes nicht unterstützt.

Die von Ihnen gewählte Lösung bestimmt die Modi, in denen Sie das Programm verwenden können:

- Wenn Sie über eine Lizenz für Kaspersky Endpoint Security verfügen, können Sie das Programm im Standard-Modus verwenden.
- Wenn Sie über eine Lizenz für Kaspersky Security for Virtualization Light Agent verfügen, können Sie das Programm im Light Agent-Modus verwenden.
- Wenn Sie über eine Lizenz für Kaspersky Endpoint Detection and Response Expert (on-premise) verfügen, können Sie das Programm im EDR-Agent-Modus verwenden.

Die Bereitstellung des Programms hängt vom ausgewählten Modus ab.

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

2 Umgebung vorbereiten

Führen Sie abhängig von Ihrer Infrastruktur die erforderlichen vorbereitenden Aktionen aus.

3 Auswahl des Mechanismus zum Abfangen von Systemereignissen

Wenn das Betriebssystem Ihres Geräts fanotify unterstützt, können Sie während der Installation auswählen, welcher Mechanismus zum Abfangen von Systemereignissen verwendet werden soll.

4 Programmpakete vorbereiten

Laden Sie die Dateien herunter, die für die Installation des Programms erforderlich sind. Welche Dateien Sie benötigen, hängt vom Betriebssystem des geschützten Geräts und von der Bereitstellungsmethode des Programms ab.

5 Vorbereitende Aktionen in Kaspersky Security Center

Führen Sie vorbereitende Aktionen in Kaspersky Security Center aus. Wir empfehlen, Kaspersky Security Center für die zentrale Verwaltung des Schutzes Ihres Unternehmens zu verwenden. Kaspersky Security Center ist außerdem erforderlich, wenn Sie Kaspersky Endpoint Security im EDR-Agent-Modus oder im Light Agent-Modus verwenden werden.

6 Programm installieren

Installieren Sie das Programm auf den Geräten mit der Methode, die den Anforderungen Ihres Unternehmens entspricht:

- Programm über Kaspersky Security Center installieren
- App über die Befehlszeile installieren

7 Zusätzliche Konfigurationsschritte nach der Installation unter bestimmten Betriebssystemen

Für einige Linux-Betriebssysteme ist nach der Installation von Kaspersky Endpoint Security eine zusätzliche Konfiguration erforderlich.

Modi und Bereitstellungsschemata

Kaspersky Endpoint Security ist Bestandteil vieler Kaspersky-Lösungen. Ihre Wahl der Lösung bestimmt den Betriebsmodus und das Bereitstellungsschema des Programms.

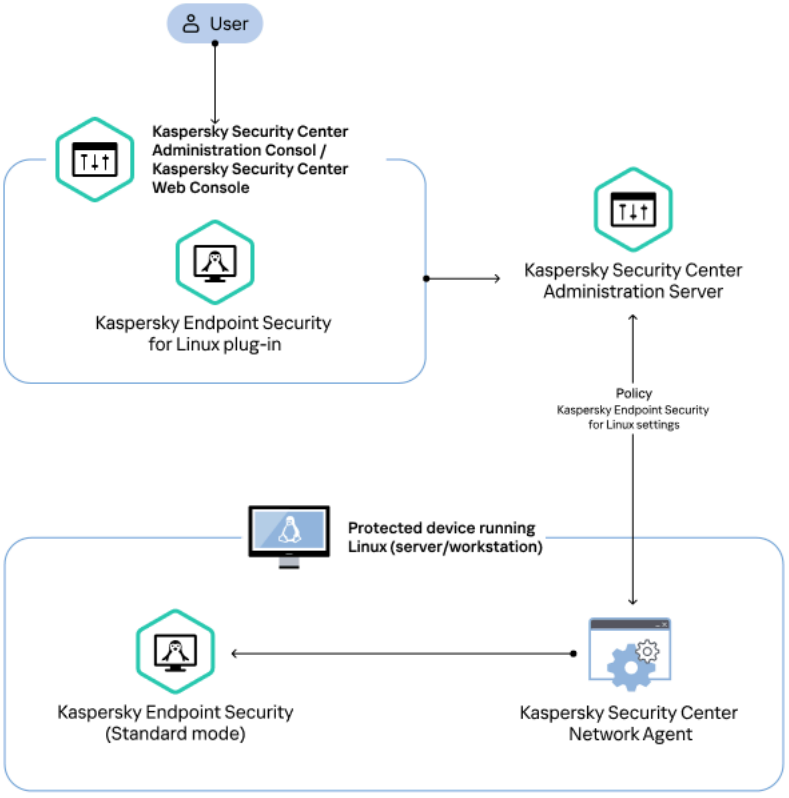
Standard-Modus

Der Standard-Modus des Programms. Kaspersky Endpoint Security bietet Linux-Workstations und -Servern umfassenden Schutz vor verschiedenen Arten von Bedrohungen, Netzwerkangriffen und Betrug.

In diesem Modus verwendet das Programm Komponenten für den Schutz und die Kontrolle von Geräten wie Schutz vor bedrohlichen Dateien oder Verhaltensanalyse sowie integrierte Agenten, um vor komplexen Bedrohungen und gezielten Angriffen zu schützen.

In diesem Modus können Sie das Programm als Teil der Lösungen von Kaspersky EPP (Endpoint Protection Platform) installieren. Kaspersky Endpoint Security im Standard-Modus ist beispielsweise Teil von Kaspersky Endpoint Security for Business.

Das gängigste Bereitstellungsschema von Kaspersky Endpoint Security ist die zentrale Bereitstellung über Kaspersky Security Center. Auf jedem geschützten Gerät müssen Sie Kaspersky Endpoint Security und die Komponente Kaspersky Security Center Administrationsagent installieren. Diese Komponente verbindet Geräte mit dem Kaspersky Security Center Administrationsserver und ermöglicht die Verwaltung von Geräten mithilfe von Kaspersky Security Center.



Bereitstellungsschema für Kaspersky Endpoint Security im Standard-Modus

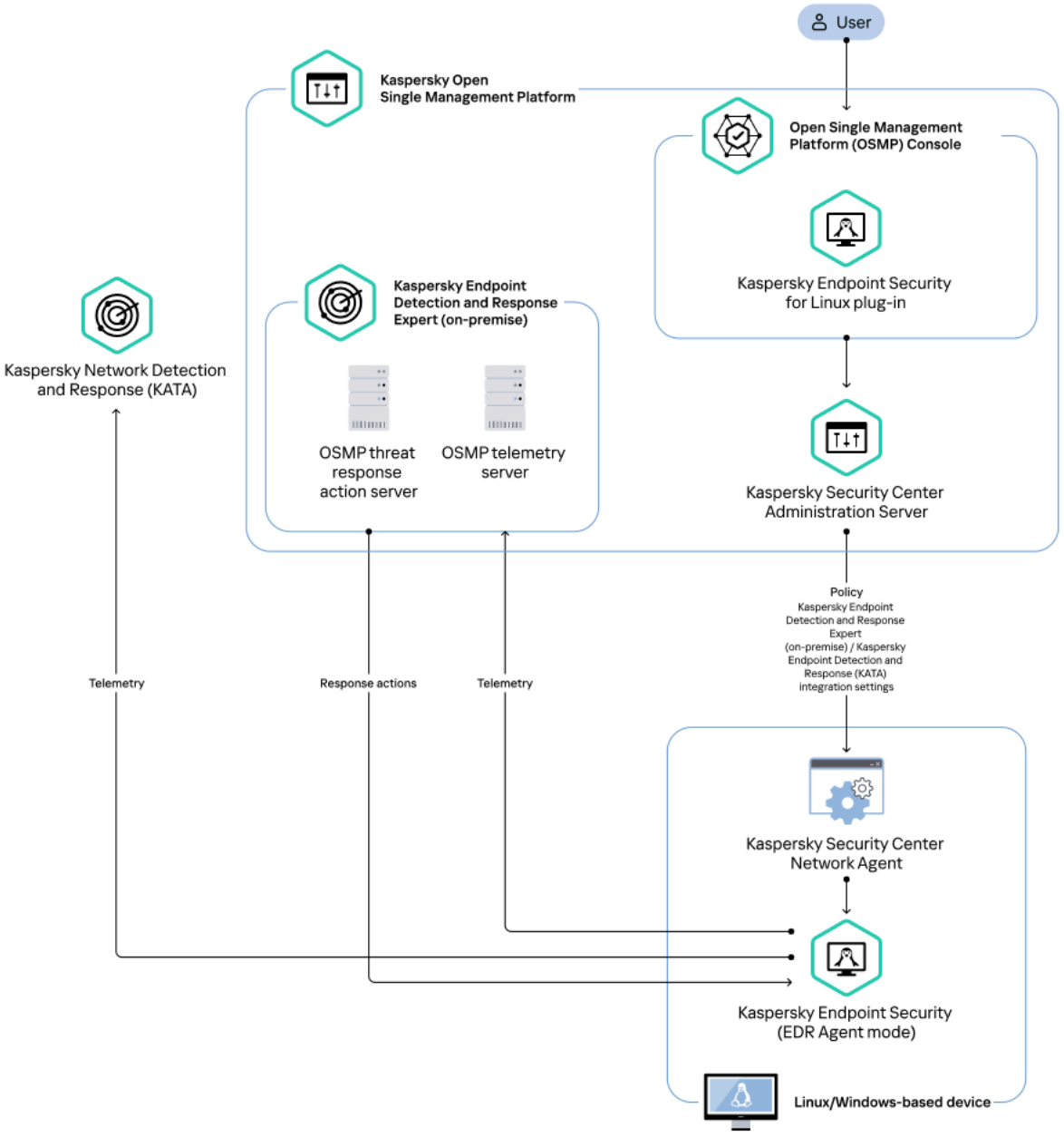
Modus des Endpoint Detection and Response Agent (EDR Agent)

Dieser Modus ermöglicht die Bereitstellung von Kaspersky-Lösungen für Detection and Response zusammen mit Antiviren-Lösungen von Drittanbietern. Zu den Lösungen für Detection and Response gehören:

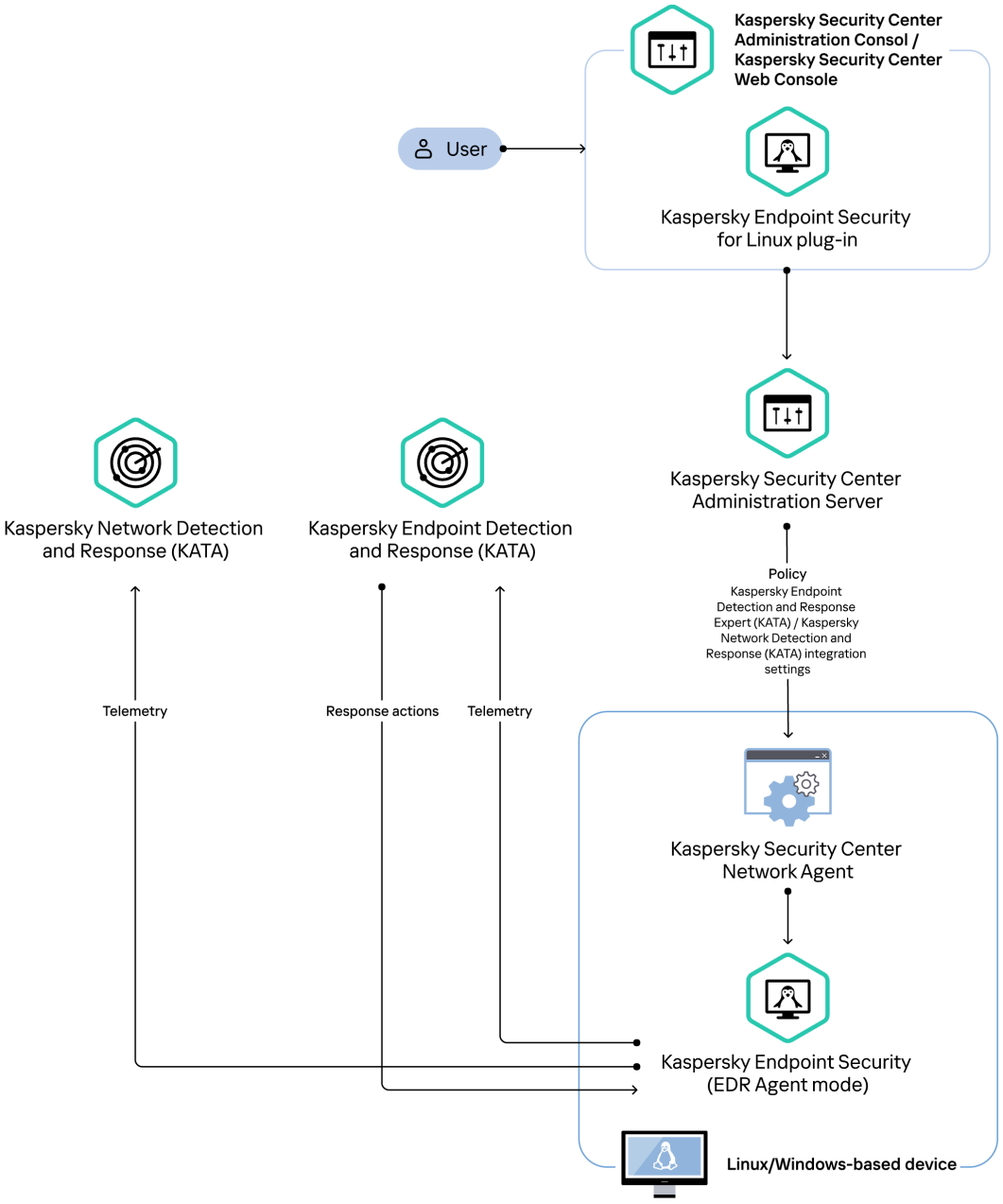
- Kaspersky Endpoint Detection and Response Expert (on-premise) auf der Open Single Management Platform (im Weiteren auch als „OSMP“ bezeichnet).
- Kaspersky Endpoint Detection and Response und Kaspersky Network Detection and Response auf der Kaspersky Anti Targeted Attack Platform (im Folgenden auch „KATA“ genannt).

Im EDR Agent-Modus sind Komponenten für den Schutz und die Kontrolle wie Schutz vor bedrohlichen Dateien oder Schutz vor Web-Bedrohungen nicht verfügbar. Eine Antiviren-Anwendung eines Drittanbieters schützt das Gerät. Der EDR-Agent überwacht kontinuierlich die auf diesen Geräten ausgeführten Prozesse, das Öffnen von Netzwerkverbindungen und Änderungen an Dateien und interagiert mit Lösungen für Detection and Response, um vor komplexen Bedrohungen und gezielten Angriffen zu schützen.

Damit Kaspersky Endpoint Security im EDR Agent-Modus betrieben werden kann, müssen Sie die entsprechende Infrastruktur bereitstellen. Weitere Informationen finden Sie in der Hilfe zu der von Ihnen ausgewählten Detection and Response-Lösung. Weitere Informationen zu den Besonderheiten des EDR-Agent-Modus finden Sie im Artikel Bekannte Probleme und Einschränkungen.



Bereitstellungsschema für Kaspersky Endpoint Security im EDR Agent-Modus zusammen mit Kaspersky Endpoint Detection and Response Expert (on-premise)



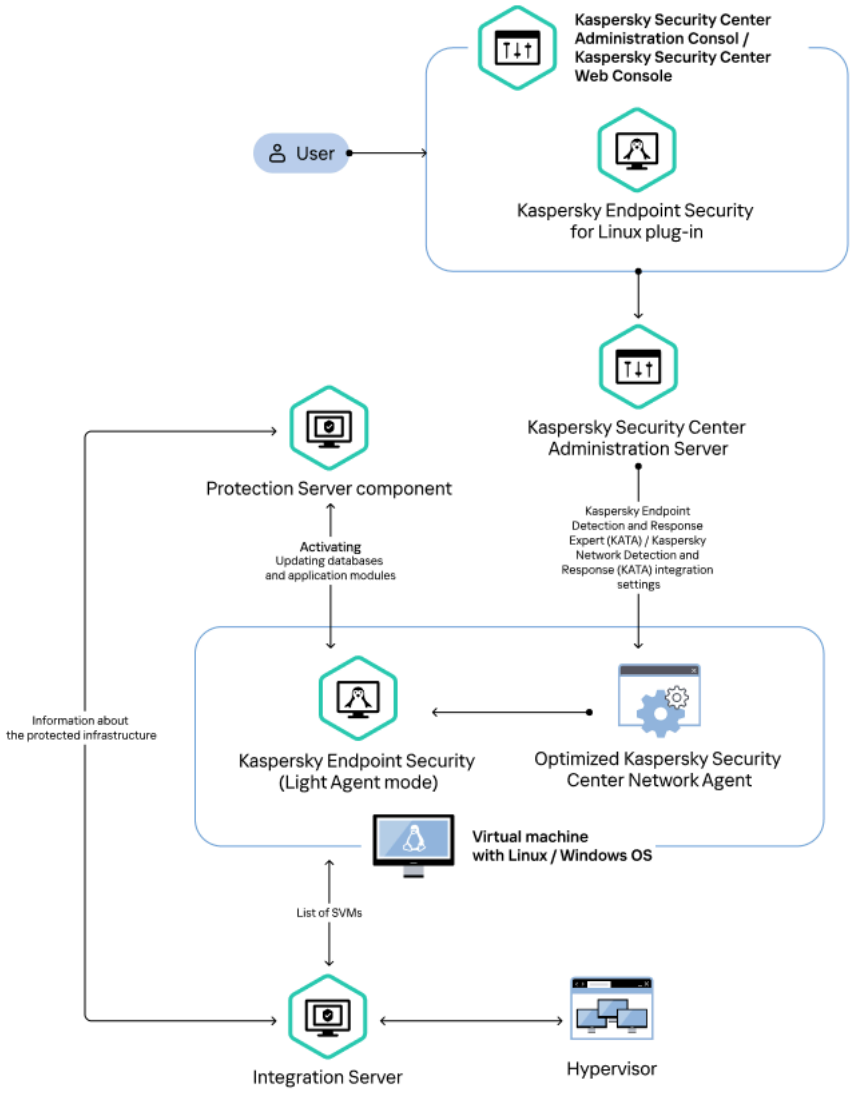
Bereitstellungsschema für Kaspersky Endpoint Security im EDR Agent-Modus zusammen mit Kaspersky Endpoint Detection and Response und Kaspersky Network Detection and Response

Light Agent-Modus

Kaspersky Endpoint Security im Light Agent-Modus ist Teil der Lösung Kaspersky Security for Virtualization Light Agent zum Schutz virtueller Maschinen, auf denen Linux-Gastbetriebssysteme ausgeführt werden.

In diesem Modus stehen die gleichen Schutz- und Kontrollkomponenten zur Verfügung wie im Standard-Modus. Der Unterschied besteht darin, dass durch eine spezielle Komponente der Lösung, die auf einer separaten virtuellen Maschine, der SVM (Secure Virtual Machine), installiert ist, Objekte auf Viren und andere Malware untersucht, Lizenzschlüssel hinzugefügt sowie Datenbanken und Module aktualisiert werden. Dies trägt zur Entlastung des Hypervisors bei, da das Programm im Light Agent-Modus zum Schutz der Infrastruktur die Ressourcen der SVM anstelle der Ressourcen virtueller Maschinen verwendet.

Damit Kaspersky Endpoint Security im Light Agent-Modus betrieben werden kann, müssen Sie die entsprechende Infrastruktur bereitstellen; weitere Informationen finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent. Weitere Informationen zu den Besonderheiten des EDR-Agent-Modus finden Sie im Artikel Bekannte Probleme und Einschränkungen.



Bereitstellungsschema für Kaspersky Endpoint Security im Light Agent-Modus

Nachdem Sie den Programmmodus ausgewählt haben, können Sie zum Bereitstellungsszenario zurückkehren und mit dem Schritt Umgebung vorbereiten fortfahren.

Umgebung für die Programminstallation vorbereiten

Infrastruktur vorbereiten

Kaspersky Security Center

Wenn Sie das Programm zentral mithilfe von Kaspersky Security Center verwalten möchten, installieren Sie Kaspersky Security Center in Ihrer Infrastruktur. Wenn Sie Kaspersky Security Center Windows bereits installiert haben und die Migration zu Kaspersky Security Center Linux planen, gehen Sie gemäß folgender Anleitung vor: Daten nach Kaspersky Security Center Linux migrieren.

Kaspersky Endpoint Security im EDR Agent-Modus

Damit Kaspersky Endpoint Security im EDR Agent-Modus betrieben werden kann, müssen Sie die entsprechende Infrastruktur bereitstellen. Weitere Informationen finden Sie in der Hilfe zu der von Ihnen ausgewählten Detection and Response-Lösung.

Kaspersky Endpoint Security im Light Agent-Modus

Damit Kaspersky Endpoint Security im Light Agent-Modus ausgeführt werden kann, müssen Sie die Lösung Kaspersky Security for Virtualization Light Agent bereitstellen:

1. Installieren Sie die Komponenten der Lösung Kaspersky Security for Virtualization Light Agent, nämlich den Integrationsserver und den Schutzserver.

2. Bereiten Sie den Schutzserver für den Betrieb vor, indem Sie die Lösung aktivieren und die Datenbanken-Updates für den Schutzserver und die Light Agents konfigurieren.

   Weitere Informationen zur Installation und Konfiguration der Lösungskomponenten finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

3. Stellen Sie sicher, dass die virtuellen Maschinen, die Sie schützen möchten, die Anforderungen für den Light Agent-Modus erfüllen.

4. 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. Die vom Light Agent verwendeten Ports sind in der Hilfe zu Kaspersky Security for Virtualization Light Agent aufgeführt.

Der Light Agent-Modus von Kaspersky Endpoint Security wird auf Geräten mit Arm-Architektur und auf Geräten mit Elbrus-CPU nicht unterstützt.

Gerät für die Installation vorbereiten

- Überprüfen Sie, ob Ihr Gerät die Hardware- und Softwareanforderungen des Programms erfüllt.

- Wenn Sie Kaspersky Endpoint Security im Standard-Modus oder im Light Agent-Modus installieren möchten, stellen Sie sicher, dass auf Ihrem Gerät keine Antiviren-Software von Drittanbietern installiert ist. Im EDR Agent-Modus kann Kaspersky Endpoint Security zusammen mit dem Dr. Web-Antivirenprogramm ausgeführt werden.

- Stellen Sie sicher, dass Kaspersky Endpoint Agent für Linux nicht auf Ihrem Gerät installiert ist. Wenn Kaspersky Endpoint Agent für Linux installiert ist, deinstallieren Sie ihn.

- Stellen Sie sicher, dass das Dienstprogramm iptables auf Ihrem Gerät installiert ist. Das Programm benötigt das Dienstprogramm iptables, um den Netzwerkverkehr abzufangen.

- Stellen Sie sicher, dass root der Eigentümer der folgenden Verzeichnisse ist und dass nur der Eigentümer Schreibzugriff hat: /var, /var/opt, /opt, /usr/bin, /usr/lib, /usr/lib64. Dies ist erforderlich, damit das Programm gestartet werden und ordnungsgemäß funktionieren kann.

- Während das Programm ausgeführt wird, verwendet das Betriebssystem möglicherweise deutlich mehr Dateideskriptoren. Stellen Sie sicher, dass der Grenzwert für die Anzahl der Deskriptoren ausreichend hoch ist. Um die Obergrenze zu überprüfen, führen Sie folgenden Befehl aus: `cat /proc/sys/fs/file-max`. Im Allgemeinen empfehlen wir, den Grenzwert zu deaktivieren, indem Sie `fs.file-max=9223372036854775807` in der Datei /etc/sysctl.conf angeben. Nachdem Sie diese Änderung vorgenommen haben, starten Sie das Betriebssystem neu.

- Stellen Sie sicher, dass `kernel.yama.ptrace_scope=0` im Betriebssystem. Andere Werte des Parameters `kernel.yama.ptrace_scope` können sich auf den Betrieb von Kaspersky Endpoint Security auswirken. Weitere Informationen finden Sie im Abschnitt Bekannte Probleme und Einschränkungen.

Zusätzlich für die Installation der grafischen Benutzeroberfläche des Programms:

- Die Version des Pakets kesl-gui, das Sie installieren, muss mit der Version Ihres Pakets kesl übereinstimmen.

- Damit die grafische Benutzeroberfläche von Kaspersky Endpoint Security ordnungsgemäß funktioniert, muss das Dienstprogramm Zenity in Ihrem Betriebssystem installiert sein.

- Wenn Ihr Gerät Zugriff auf die Repositorys des Paketmanagers hat, werden alle erforderlichen Abhängigkeiten während der Installation der grafischen Benutzeroberfläche des Programms automatisch installiert. Wenn sich das Gerät in einem privaten Segment befindet und keinen Zugriff auf die Repositorys des Paketmanagers hat:

  1. Überprüfen Sie die Liste der Abhängigkeiten auf einem Referenzgerät (libice6, libsm6, zlib1g, kesl).

  2. Führen Sie eine der folgenden Aktionen aus:

     - Laden Sie vor der Installation der grafischen Benutzeroberfläche die Pakete auf alle Geräte herunter und installieren Sie sie anschließend mithilfe des Paketmanagers.

     - Stellen Sie sicher, dass die Pakete während der Installation der grafischen Benutzeroberfläche auf die Geräte heruntergeladen werden.

Zusätzlich für die Unterstützung des MMC-Plug-ins

Wenn Sie das Programm mithilfe der Kaspersky Security Center Verwaltungskonsole verwalten möchten, installieren Sie Microsoft® Visual C++® 2015 Redistributable Update 3 RC auf dem Gerät, auf dem der Administrationsserver installiert ist (siehe https://www.microsoft.com/en-us/download/details.aspx?id=52685). Dies ist erforderlich, damit das MMC-Verwaltungs-Plug-in von Kaspersky Endpoint Security funktioniert.

Zusätzlich für bestimmte Betriebssysteme

Astra Linux im Modus der geschlossenen Softwareumgebung

Installation des Kompatibilitätspakets

In den folgenden Fällen müssen Sie das Kompatibilitätspaket installieren:

- Vor der Installation des Programms im Modus der geschlossenen Softwareumgebung.
- Wenn die Anwendung bereits installiert ist und das Betriebssystem in den Modus der geschlossenen Softwareumgebung versetzt wird.

```
Installationspaket
```

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

Dadurch kann die Anwendung unter den Betriebssystemen Astra Linux Special Edition (Updates 4.7 für die Arm-Architektur, 1.6, 1.7 und 1.8) im Modus der geschlossenen Softwareumgebung ausgeführt werden.

Erneutes Zulassen von ptrace

In Astra Linux Betriebssystemen ist das Verbot von ptrace-Protokollierung (Disable ptrace capability) standardmäßig aktiviert, das sich auf die Ausführung der Anwendung 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**).

SUSE Linux Enterprise Server 15

Vor der Installation der Anwendung auf einem Gerät mit dem Betriebssystem SUSE Linux Enterprise Server 15 muss das Paket insserv-compat installiert werden.

ALT SP im Modus der geschlossenen Softwareumgebung

Vor der Installation der Anwendung auf einem Gerät mit dem Betriebssystem ALT SP im Modus der geschlossenen Softwareumgebung:

1. Deaktivieren Sie den Modus der geschlossenen Softwareumgebung:

   ```
   integrity-remover
   ```

2. Erstellen Sie eine kesl-Gruppe für weitere Änderungen an der IMA-Richtlinie:

   ```
   groupadd kesl
   ```

3. Ermitteln Sie die eindeutige Kennung (GID) der erstellten Gruppe:

   ```
   cat /etc/group | grep kesl
   ```

4. Bearbeiten Sie die IMA-Richtlinie mithilfe des Dienstprogramms, um die kesl-Gruppe von der Integritätsprüfung der Programmkomponenten auszuschließen und sicherzustellen, dass das Programm ordnungsgemäß funktioniert. Gehen Sie dazu folgendermaßen vor:

   a. Kopieren Sie die Datei /usr/share/integrity/policy:

      ```
      cp /usr/share/integrity/policy /etc/integrity/policy
      ```

b. Öffnen Sie die Datei /etc/integrity/policy zur Bearbeitung in einem Texteditor (z. B. vim):

```
vim /etc/integrity/policy
```

c. Fügen Sie nach der Zeile `dont_measure fsmagic=0xf97cff8c` (normalerweise ist dies die letzte Zeile des Abschnitts `dont_measure`) folgende Zeile hinzu:

```
dont_measure fgroup=<GID>
```

wobei `<GID>` eine eindeutige ID der in Schritt 2 dieser Anleitung erstellten Gruppe ist.

d. Fügen Sie nach der Zeile `dont_appraise fsmagic=0x27e0eb` (normalerweise ist dies die letzte Zeile des Abschnitts `dont_appraise`) folgende Zeile hinzu:

```
dont_appraise fgroup=<GID>
```

wobei `<GID>` eine eindeutige ID der in Schritt 2 dieser Anleitung erstellten Gruppe ist.

e. Speichern Sie die vorgenommenen Änderungen.

5. Ändern Sie in der Datei "/usr/sbin/integrity-sign" die Funktion "list_all_files" in der Weise, dass die Anwendung "Kaspersky Endpoint Security" in die Allow-Liste der Anwendungen aufgenommen wird, die im Modus für geschlossenen Softwareumgebungen ausgeführt werden dürfen. Gehen Sie dazu folgendermaßen vor:

a. Öffnen Sie die Datei /usr/sbin/integrity-sign zur Bearbeitung in einem Texteditor (z. B. vim):

```
vim /usr/sbin/integrity-sign
```

b. Suchen Sie die Funktion "list_all_files" und fügen Sie im Funktionskörper in den Zeilen, die mit `find -P` beginnen, am Ende jeder Verzeichnisliste die Anwendungsverzeichnisse von Kaspersky Endpoint Security hinzu: "/var/opt" und "/opt".

c. Speichern Sie die vorgenommenen Änderungen.

Starten Sie während der Erstkonfiguration der Anwendung kein Datenbanken-Update.

Führen Sie nach Abschluss der Programminstallation die notwendigen Schritte zur Inbetriebnahme aus.

OSnova

Wenn Sie die Anwendung mithilfe von Kaspersky Security Center installieren und verwalten möchten, bereiten Sie vor der Installation der Anwendung das Gerät für die Installation des Administrationsagenten vor:

1. Öffnen Sie die Datei /usr/lib/systemd/logind.conf.d/10-enable-kill-user-processes.conf zur Bearbeitung und kommentieren Sie im Abschnitt `[Login]` die Zeile KillUserProcesses=yes aus.

```
#KillUserProcesses=yes
```

2. Öffnen Sie die Datei /usr/lib/NESS/pam-user-session zur Bearbeitung und kommentieren Sie die Zeile loginctl terminate-session "$XDG_SESSION_ID" aus.

```
#loginctl terminate-session "$XDG_SESSION_ID"
```

Betriebssysteme mit SELinux-Unterstützung

Wenn das Hilfsprogramm semanage in Ihrem Betriebssystem nicht installiert ist, installieren Sie vor der Installation des Programms je nach Paketmanager das Paket policycoreutils-python oder policycoreutils-python-utils.

Das Paket policycoreutils-python-utils wird für die folgenden Typen von Paketmanagern bereitgestellt: dnf, apt und yum für Fedora, Debian, Ubuntu und RHEL und höher.

Das Paket policycoreutils-python wird für die folgenden Typen von Paketmanagern bereitgestellt: yum und CentOS/RHEL und älter.

Kylin OS

Vor der Installation der Anwendung auf einem Gerät mit Kylin OS:

1. Deaktivieren Sie in der UKUI (Ubuntu Kylin User Interface) Firewall. Wechseln Sie dazu zum Abschnitt **Kylin-Sicherheitscenter** → **Firewall und Netzwerkschutz** und deaktivieren Sie unter **Firewall** die Umschalter **Öffentliches Netzwerk** und **Privates Netzwerk**.

2. Deaktivieren Sie in der UKUI die Programm-Netzwerkkontrolle. Wechseln Sie dazu zum Abschnitt **Kylin-Sicherheitscenter** → **Firewall und Netzwerkschutz** und wählen Sie unter **Programm-Netzwerkkontrolle** die Option **Deaktivieren** aus.

3. Deaktivieren Sie in der UKUI die Programm-Quellprüfung. Wechseln Sie dazu zum Abschnitt **Kylin-Sicherheitscenter** → **Programmschutz** und wählen Sie unter **Programm-Quellprüfung** die Option **Deaktivieren** aus.

4. Deaktivieren Sie den KYSEC-Sicherheitsmechanismus. Führen Sie dazu im Terminal die folgenden Aktionen aus:

   a. Überprüfen Sie den aktuellen Status:

   ```
   getstatus
   ```

   b. Deaktivieren Sie den KYSEC-Sicherheitsmechanismus:

   ```
   setstatus disable -p
   ```

   c. Stellen Sie sicher, dass der KYSEC-Sicherheitsmechanismus deaktiviert ist:

   ```
   getstatus
   ```

5. Deinstallieren Sie das integrierte Antivirenprogramm. Führen Sie dazu im Terminal den folgenden Befehl aus:

```
sudo dpkg -P pksav
```

6. Wenn das Antivirenprogramm Qaxsafe auf Ihrem Gerät installiert ist, müssen Sie es deinstallieren. Gehen Sie dazu folgendermaßen vor:

   a. Deaktivieren Sie den Selbstschutz:

      1. Suchen Sie im Infobereich der Taskleiste nach dem Programmsymbol und doppelklicken Sie auf das Programmsymbol, um das Kontextmenü zu öffnen.

      2. Wählen Sie im Kontextmenü **Einstellungen** → **Schutz-Center**.

      3. Daraufhin wird ein Fenster geöffnet. Deaktivieren Sie in diesem Fenster das Kontrollkästchen **Selbstschutz aktivieren** und geben Sie ein Kennwort ein, wenn Sie dazu aufgefordert werden.

   b. Deinstallieren Sie das Qaxsafe-Antivirenprogramm. Führen Sie dazu im Terminal den folgenden Befehl aus:

   ```
   sudo dpkg -P qaxsafe
   ```

   c. Löschen Sie alle verbleibenden Dateien. Führen Sie dazu im Terminal den folgenden Befehl aus:

   ```
   sudo rm -rf /opt/qaxsafe
   ```

Betriebssysteme, die fanotify nicht unterstützen

Bevor Sie mit der Installation des Programms fortfahren, stellen Sie sicher, dass Folgendes auf dem Gerät 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

Nützliche Artikel

Beheben von Problemen unter Kylin OS

Nach der Vorbereitung der Umgebung für die Installation können Sie zum Bereitstellungsszenario zurückkehren und mit dem Schritt Auswahl des Mechanismus zum Abfangen von Systemereignissen fortfahren.

Auswahl des Mechanismus zum Abfangen von Systemereignissen

Um eine ordnungsgemäße Funktion zu gewährleisten, muss das Programm Systemereignisse für Dateivorgänge und Prozessstarts abfangen. Das Abfangen von Systemereignissen ist in allen Programmmodi erforderlich (Standard-Modus, Light Agent-Modus und EDR-Agent-Modus). Wenn das Abfangen von Systemereignissen von der Anwendung nicht verwendet wird, findet keine Dateiuntersuchung in Echtzeit statt. Dies reduziert die Schutzstufe des Geräts.

Mechanismus zum Abfangen von Systemereignissen

Das Programm kann die folgenden Mechanismen verwenden, um Systemereignisse abzufangen:

- **Abfangmechanismus auf Basis der fanotify-Technologie.** *Fanotify* ist ein Subsystem des Linux-Kernels, das Ereignisse im Dateisystem überwacht (z. B. das Öffnen, Lesen, Schreiben oder Schließen von Dateien) und es Programmen ermöglicht, diese in Echtzeit abzufangen.

- **Abfangmechanismus auf Basis des aktualisierbaren Kernel-Moduls.** Das *aktualisierbare Kernel-Modul* arbeitet mit dem Mechanismus zum Abfangen von Systemereignissen zusammen, der auf der fanotify-Technologie basiert. Dadurch können Sie das Abfangen von Dateivorgängen und Prozessstarts durch Kaspersky Endpoint Security optimieren, indem Systemereignisse in kernel space und nicht in user space verarbeitet werden. Das aktualisierbare Kernel-Modul fängt Dateivorgänge beim Öffnen, Umbenennen und Ändern von Dateien ab. Die Leistung des Programms wird durch den Cache für die Untersuchungsergebnisse von Dateien und Prozessen erhöht.

  Das aktualisierbare Kernel-Modul wird auch für die folgenden Aufgaben und Komponenten verwendet:

  - Schutz vor bedrohlichen Dateien
  - Schutz vor Verschlüsselung
  - Exploit-Prävention
  - Verhaltensanalyse
  - Programmkontrolle
  - Ausführungsprävention für Objekte (bei der Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) und Kaspersky Endpoint Detection and Response Optimum)

  Bei Verwendung des aktualisierbaren Kernel-Moduls können Sie globale Ausnahmen jetzt noch präziser anpassen. Mit dem auf der fanotify-Technologie basierenden Abfangmechanismus lässt sich das Abfangen von Dateivorgängen für die angegebenen Mount-Punkte vollständig ausschließen. Das aktualisierbare Kernel-Modul erlaubt das Ausschließen bestimmter, auf dem Gerät gemounteter lokaler Verzeichnisse oder Netzwerkverzeichnisse.

  Das aktualisierbare Kernel-Modul ist im Lieferumfang der Anwendung enthalten.

- **Kernel-Modul für den Schutz vor bedrohlichen Dateien auf einem Betriebssystem ohne fanotify**. Wenn das Betriebssystem auf dem Gerät die fanotify-Technologie nicht unterstützt (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6), kompiliert das Programm ein spezielles Modul und verwendet es, um Systemereignisse abzufangen. Dieses Modul wird beim Start des Schutzes vor bedrohlichen Dateien automatisch kompiliert, sofern die zur Kompilierung erforderlichen Pakete und Tools vorhanden sind.

So wählen Sie einen Mechanismus zum Abfangen von Systemereignissen aus

Wenn das Betriebssystem fanotify unterstützt, können Sie bei der Bereitstellung des Programms einen Mechanismus zum Abfangen von Systemereignissen auswählen: nur fanotify oder aktualisierbares Kernel-Modul plus fanotify. Die Standardeinstellung ist fanotify. Nach der Installation können Sie den Mechanismus zum Abfangen von Systemereignissen in den Programmeinstellungen ändern.

Für Betriebssysteme, von denen die fanotify-Technologie nicht unterstützt wird, steht die Auswahl des Abfangmechanismus nicht zur Verfügung.

Die Anwendung kann den auf dem aktualisierbaren Kernel-Modul basierenden Abfangmechanismus verwenden, wenn das Betriebssystem die Anforderungen an die Installation des Kernel-Moduls erfüllt.

Installationsvoraussetzungen für das aktualisierbare Kernel-Modul

Um das aktualisierbare Kernel-Modul zu installieren und auszuführen, muss auf dem Gerät eines der folgenden 64-Bit-Betriebssysteme installiert sein:

- Astra Linux Special Edition RUSB.10015-01 (reguläres Update 1.6.5, 1.6.6).
- Astra Linux Special Edition RUSB.10015-01 (reguläres Update 1.7.3, 1.7.4, 1.7.6, 1.7.7, 1.7.8, 1.7.9).
- Astra Linux Special Edition RUSB.10015-01 (reguläres Update 1.8.2, 1.8.3, 1.8.4, 1.8.5).

  Wenn Kaspersky Endpoint Security im Standard-Modus verwendet wird, kann das aktualisierbare Kernel-Modul auf Geräten mit Astra Linux-Betriebssystemen im Modus für geschlossene Softwareumgebungen eingesetzt werden.

- CentOS 7.x.
- CentOS 8.x.
- Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12
- Red Hat Enterprise Linux 7,4.
- Red Hat Enterprise Linux 8.10
- SberLinux 8.10
- SberLinux 9.0.1.
- SberLinux 9.1
- SberLinux 9.6
- SberLinux 9.7
- SberOS 3.4.
- SberOS 3.5.
- Ubuntu 16.04 LTS
- Ubuntu 18.04 LTS
- Ubuntu 20.04 LTS
- Ubuntu 22.04 LTS
- Ubuntu 24.04 LTS.

- ALT SP Workstation Release 10
- ALT SP Server Release 10
- ALT Education 10
- ALT Workstation 11
- ALT Server 11
- ALT Education 11
- RED OS 7,3.
- RED OS 8,0.
- ROSA Cobalt 7.9 Workstation
- ROSA Cobalt 7.9 Server
- ROSA Chrome 12 Workstation
- ROSA "Chrom" 12 Server

32-Bit-Betriebssysteme, Betriebssysteme für die Arm-Architektur und Betriebssysteme für die Elbrus-Architektur werden nicht unterstützt.

Bei der Ausführung des aktualisierbaren Kernel-Moduls können sowohl auf Geräten mit bestimmten Versionen des Linux-Kernels als auch bei der gleichzeitigen Verwendung einige Drittanbieter-Anwendungen Konflikte auftreten.

Möglichkeit zur Installation des aktualisierbaren Kernel-Moduls überprüfen

Die Version des aktualisierbaren Kernel-Moduls ist unabhängig von der Version von Kaspersky Endpoint Security. Die Funktionalität des aktualisierbaren Kernel-Moduls wird im Rahmen von Updates für Datenbanken und Programm-Module von Kaspersky Endpoint Security regelmäßig erweitert. Daher ist die oben aufgeführte Liste der unterstützten Betriebssysteme möglicherweise nicht vollständig. Um zu überprüfen, ob Ihr Gerät die Voraussetzungen für die Installation des aktualisierbaren Kernel-Moduls erfüllt, verwenden Sie das Kaspersky ULKM-Tool.

So prüfen Sie remote mithilfe der Web Console oder der Verwaltungskonsole

1. Laden Sie das Archiv "ulkmtool.zip" von der Seite zum Anwendungs-Download im Abschnitt **Kaspersky Endpoint Security für Linux** herunter.
2. Erstellen Sie ein Installationspaket für das Tool.

So erstellen Sie ein Installationspaket in der Web Console:

1. Verschieben Sie das heruntergeladene Archiv "ulkmtool.zip" in einen Ordner, auf den der Administrationsserver von Kaspersky Security Center zugreifen kann.
2. 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.
3. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Pakete wird gestartet.
4. Wählen Sie zum Erstellen des Installationspakets die Methode **Installationspaket aus Datei erstellen**.
5. Geben Sie den Namen des neuen Installationspakets ein, klicken Sie auf die Schaltfläche **Durchsuchen** und geben Sie den Pfad zum heruntergeladenen Archiv "ulkmtool.zip" an.
6. Schließen Sie den Assistenten ab.

Das Installationspaket wird erstellt und der Liste mit Installationspaketen hinzugefügt.

So erstellen Sie ein Installationspaket in der Verwaltungskonsole:

1. Entpacken Sie das Archiv "ulkmtool.zip" in einen Ordner, auf den der Administrationsserver von Kaspersky Security Center zugreifen kann.
2. Wählen Sie in der Konsolenstruktur den Punkt **Erweitert → Remote-Installation → Installationspakete** aus.

   Es öffnet sich eine Liste mit den verfügbaren Installationspaketen auf dem Administrationsserver.
3. Klicken Sie auf **Installationspaket erstellen**.

   Der Assistent für neue Pakete wird gestartet.
4. Klicken Sie auf die Schaltfläche **Installationspaket für eine Kaspersky-Anwendung erstellen**.
5. Geben Sie den Namen des neuen Installationspakets ein und wechseln Sie zum nächsten Schritt des Assistenten.
6. Klicken Sie auf die Schaltfläche **Durchsuchen** und geben Sie den Pfad zur Datei "ulkmtool.kud" an. Die Datei befindet sich in dem Ordner, in den Sie das Archiv "ulkmtool.zip" extrahiert haben.

   Wechseln Sie zum nächsten Schritt des Assistenten.
7. Warten Sie, bis die Datei hochgeladen ist, und beenden Sie den Assistenten.

Das Installationspaket wird erstellt und der Liste mit Installationspaketen hinzugefügt.

3. Installieren Sie den Kaspersky Security Center Administrationsagenten auf den Geräten, für die Sie prüfen möchten, ob sie die Anforderungen an die Installation des aktualisierbaren Kernel-Moduls erfüllen. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security Center.

4. Erstellen und starten Sie in der Kaspersky Security Center Web Console oder in der Verwaltungskonsole eine Aufgabe zur Remote-Installation auf den Geräten, bei denen Sie prüfen möchten, ob sie die Voraussetzungen für das aktualisierbare Kernel-Modul erfüllen. Wählen Sie in den Parametern der Aufgabe das von Ihnen erstellte Installationspaket aus.

   Nach der Aufgabenausführung wird für jedes Gerät, auf dem die Aufgabe ausgeführt wurde, angegeben, ob das Gerät die Installation und die Ausführung des aktualisierbaren Kernel-Moduls unterstützt.

Basierend auf den Ergebnissen der Aufgabe wird jedem Gerät automatisch ein Tag zugewiesen:

- *UpdatableKernelModule=No* – das Gerät unterstützt die Installation des aktualisierbaren Kernel-Moduls nicht.
- *UpdatableKernelModule=Yes* – das Gerät erfüllt die Anforderungen an die Installation und Ausführung des aktualisierbaren Kernel-Moduls.

Sie können diese Tags nutzen, um Geräteauswahlen zu erstellen. Sie können beispielsweise alle Geräte auswählen, welche die Anforderungen an das aktualisierbare Kernel-Modul erfüllen und anschließend Kaspersky Endpoint Security mit dem aktualisierbaren Kernel-Modul auf ihnen installieren.

So prüfen Sie lokal auf dem Gerät

1. Laden Sie das Archiv "ulkmtool.zip" von der Seite zum Anwendungs-Download im Abschnitt **Kaspersky Endpoint Security für Linux** herunter.
2. Installieren Sie den Kaspersky Security Center Administrationsagenten auf den Geräten, für die Sie prüfen möchten, ob sie die Anforderungen an die Installation des aktualisierbaren Kernel-Moduls erfüllen. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security Center.
3. Führen Sie das Dienstprogramm Kaspersky ULKM tool lokal auf den Geräten aus, die Sie untersuchen möchten.

   ```
   ulkmtool --check remote
   ```

4. Überprüfen Sie den Rückgabecode.

   ```
   echo $?
   ```

   Das Tool gibt in der Befehlszeile die folgenden Codes zurück:

   0 = Erfolg bedeutet, dass das Gerät die Voraussetzungen für die Installation und Ausführung des aktualisierbaren Kernel-Moduls erfüllt.

   1 = Nicht unterstützt bedeutet, dass das Gerät die Installation des aktualisierbaren Kernel-Moduls nicht unterstützt.

Status des aktualisierbaren Kernel-Moduls prüfen

In der Kaspersky Security Center Web Console oder in der Verwaltungskonsole können Sie den Status des aktualisierbaren Kernel-Moduls auf Geräten mit Kaspersky Endpoint Security überprüfen. Dazu können Sie die den Geräten zugewiesenen Tags anzeigen:

- *UpdatableKernelModule=Use* – auf dem Gerät ist ein aktualisierbares Kernel-Modul installiert und wird ausgeführt.
- *UpdatableKernelModule* = *Error* – auf dem Gerät ist das aktualisierbare Kernel-Modul installiert, aber beim Starten des Moduls ist ein Fehler aufgetreten. Das Modul funktioniert nicht.

Weitere Informationen über das Anzeigen von Tags, die Geräten zugewiesen sind, finden Sie in der Hilfe zu Kaspersky Security Center.

Unterstützung für Secure Boot

Das aktualisierbare Kernel-Modul unterstützt Secure Boot. Um den Abfangmechanismus auf Basis des aktualisierbaren Kernel-Moduls auf Betriebssystemen mit aktiviertem Secure Boot zu verwenden, müssen Sie das öffentliche Zertifikat von Kaspersky Endpoint Security, mit dem das Modul signiert ist, dem Betriebssystem hinzufügen und anschließend das Betriebssystem neu starten.

Zertifikat herunterladen

Beispiel für das Hinzufügen eines Zertifikats unter Ubuntu

1. Stellen Sie sicher, dass Secure Boot in Ihrem Betriebssystem aktiviert ist:

   ```
   mokutil --sb-state
   ```

2. Fügen Sie das heruntergeladene Zertifikat mithilfe des Tools mokutil zu Ihrem Betriebssystem hinzu:

   ```
   mokutil --import <path to certificate>
   ```

3. Starten Sie das Betriebssystem neu und bestätigen Sie den Zertifikatsimport im Menü des MOK-Managers.

4. Prüfen Sie mit dem folgenden Befehl, ob das aktualisierbare Kernel-Modul funktioniert:

   ```
   kesl-control --app-info
   ```

Nachdem Sie den Mechanismus zum Abfangen von Systemereignissen ausgewählt haben, können Sie zum Bereitstellungsszenario zurückkehren und mit dem Schritt Vorbereiten der Programmpakete fortfahren.

Programmpakete vorbereiten

Das *Programmpaket für Kaspersky Endpoint Security* besteht aus Dateien zur Installation und Aktualisierung des Programms sowie aus den Texten der Benutzervereinbarungen (Endbenutzer-Lizenzvertrag, Datenschutzrichtlinie und Erklärung zu Kaspersky Security Network). Sie können außerdem separat das Programmpaket herunterladen, das eine grafische Benutzeroberfläche zur komfortablen lokalen Verwaltung und Überwachung des Programms enthält.

Sie benötigen Programmpakete, um ein Installationspaket für die Bereitstellung auf Geräten im Unternehmensnetzwerk mithilfe von Kaspersky Security Center zu erstellen, sowie um das Programm über die Befehlszeile bereitzustellen.

Für die Bereitstellung mithilfe von Kaspersky Security Center benötigen Sie außerdem ein *Programmpaket für die Remote-Installation des Programms*. Dieses Programmpaket enthält die Dateien, die für die Remote-Bereitstellung des Programms erforderlich sind, sowie die Texte der Benutzervereinbarungen.

Die Texte der Benutzervereinbarungen sind auf der Kaspersky-Website (im Abschnitt **EULA**) sowie nach der Installation des Programms im Verzeichnis `/opt/kaspersky/kesl/doc/` verfügbar.

Sie können die Programmpakete für die Bereitstellung von Kaspersky Endpoint Security selbstständig oder mithilfe von Kaspersky Security Center im Schritt Erstellen eines Installationspakets auswählen.

So wählen Sie ein Programmpaket für die Bereitstellung von Kaspersky Endpoint Security aus

Die Auswahl der Programmpakete hängt von folgenden Faktoren ab:

- Version von Kaspersky Endpoint Security: zertifiziert oder nicht zertifiziert
- Bereitstellungsmethode: mithilfe von Kaspersky Security Center oder über die Befehlszeile
- Paketformat abhängig vom Betriebssystem
- Betriebssystemarchitektur und CPU-Typ
- Verwaltungsmethode für Kaspersky Endpoint Security
- Notwendigkeit der Installation der grafischen Benutzeroberfläche des Programms

1. **Bestimmen Sie, ob Ihre Programmversion zertifiziert oder nicht zertifiziert ist**

   - Wenn Sie die **zertifizierte** Version benötigen, laden Sie den Satz von Programmpaketen von der Seite Support-Lebenszyklus für Geschäftsanwendungen herunter.

     Die zertifizierte Version enthält die Hauptdateien des Programms und die Dateien der grafischen Benutzeroberfläche (das Verzeichnis `kesl`), ein Archiv für die Remote-Installation des Programms (das Verzeichnis `remote install`), das MMC-Plug-in (`SCPlugin`) und das Web-Plug-in (`web plugin`).

     Gehen Sie zu Schritt 3.

   - Wenn Sie die **nicht zertifizierte** Version benötigen, fahren Sie mit dem nächsten Schritt fort.

2 Legen Sie die Bereitstellungsmethode fest: mithilfe von Kaspersky Security Center oder über die Befehlszeile

Für die **Bereitstellung mithilfe von Kaspersky Security Center** laden Sie das Programmpaket aus einer der folgenden Quellen herunter:

- Von der Kaspersky-Website
- Durch das Erstellen einer Anfrage an den Technischen Support, wenn Sie über einen Kaspersky CompanyAccount verfügen

Für die **Bereitstellung über die Befehlszeile** laden Sie das Programmpaket von der Kaspersky-Website herunter:

- Das Hauptprogrammpaket (`Distributive`)
- Bei Bedarf das Programmpaket mit der grafischen Benutzeroberfläche (`Product GUI`)

Wenn Sie die Programmpakete von der Kaspersky-Website herunterladen möchten, benötigen Sie die folgenden Dateien:

- Das Hauptprogrammpaket (`Distributive`)
- Bei Bedarf das Programmpaket mit der grafischen Benutzeroberfläche (`Product GUI`)
- Programmpaket für die Remote-Installation des Programms mithilfe von Kaspersky Security Center (**Zusätzliches Programmpaket** → `Files for Product remote installation`)
- Programmpaket des Kaspersky Security Center Administrationsagenten (Abschnitt für die Kaspersky Security Center-Distribution → `Network agent`)

Das Programmpaket ist für alle Lokalisierungen identisch. Die Sprache von Kaspersky Endpoint Security wird bei der Erstkonfiguration des Programms ausgewählt. Die Unterstützung der Lokalisierung hängt von den Sprachen ab, die im Betriebssystem installiert sind.

3 Legen Sie das Paketformat abhängig vom Betriebssystem des geschützten Geräts fest

Betriebssystem	Paketformat
Debian, Ubuntu, Astra Linux, Linux Mint	`.deb`
Red Hat Enterprise Linux, CentOS, Oracle Linux, RED OS, SUSE Linux Enterprise, openSUSE, Rocky Linux, AlmaLinux, Betriebssysteme der ALT-Serie, GosLinux, Betriebssysteme der Rosa-Serie, Amazon Linux 2023	`.rpm`

Wenn Ihr Betriebssystem nicht aufgeführt ist, wählen Sie das Paketformat gemäß der Dokumentation zu Ihrem Betriebssystem aus.

4 Bestimmen Sie die Architektur des Betriebssystems und den CPU-Typ

CPU-Typ und Bitbreite des Betriebssystems	Programmpaket
Arm-CPU, 64-Bit-Betriebssystem	`arm64` `aarch64`
Elbrus-CPU	`e2k`
Sonstige Prozessoren, 32-Bit-Betriebssystem	`i386`

CPU-Typ und Bitbreite des Betriebssystems	Programmpaket

Sonstige Prozessoren, 64-Bit-Betriebssystem	`x86_64`
	`x64`
	`amd64`

Um das Programm Kaspersky Endpoint Security auf Betriebssystemen mit eingeschränkter Unterstützung (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6) zu installieren, wählen Sie das mit `OLD` gekennzeichnete Programmpaket aus.

Wenn die Konfigurationsdateien der Anwendung auf andere Weise geändert werden, als in der Dokumentation zur Anwendung oder in den Anleitungen der Support-Experten beschrieben, kann dies die Anwendung oder das Betriebssystem verlangsamen oder negativ beeinträchtigen. Es kann das Schutzniveau Ihres Gerätes senken und den Zugriff auf die, bzw. die Integrität der verarbeiteten Informationen, einschließlich der zusätzlich übertragenen KSN-Statistiken, beeinträchtigen.

Nachdem Sie die Programmpakete vorbereitet haben, können Sie zum Bereitstellungsszenario zurückkehren und mit dem Schritt Vorbereitende Aktionen in Kaspersky Security Center fortfahren.

Vorbereitende Aktionen in Kaspersky Security Center

Bevor Sie Kaspersky Endpoint Security installieren, empfehlen wir, in Kaspersky Security Center Folgendes zu tun.

1 Administrationsgruppen für Geräte konfigurieren

Um das Programm mithilfe von Kaspersky Security Center zu verwalten, müssen Sie die Geräte, auf denen das Programm installiert ist, in Administrationsgruppen einordnen. Standardmäßig verschiebt Kaspersky Security Center alle Geräte, auf denen der Administrationsagent installiert ist und die mit dem Administrationsserver verbunden sind, in die Gruppe **Nicht zugeordnete Geräte**.

Wir empfehlen, im Voraus Regeln für die automatische Platzierung von Geräten in Administrationsgruppen zu konfigurieren und die Geräte entsprechend ihrem Typ Gruppen zuzuweisen, indem für jeden Gerätetyp eine separate Gruppe erstellt wird. Dadurch können Sie je nach Gerät unterschiedliche Programmeinstellungen anwenden.

Sie können Geräte auch manuell in Administrationsgruppen platzieren.

2 Installation und Erstkonfiguration des Administrationsagenten

Der Administrationsagent stellt die Verbindung des Geräts mit dem Kaspersky Security Center Administrationsserver sicher. Er muss auf jedem Gerät installiert werden, das mit Kaspersky Security Center verbunden wird.

1. Bereiten Sie Ihre Linux-Geräte für die Installation des Administrationsagenten vor. Der Umfang der erforderlichen Schritte hängt vom Betriebssystem ab.

2. Führen Sie die Installation und Erstkonfiguration des Administrationsagenten durch. Anweisungen finden Sie in der Hilfe zu Kaspersky Security Center.

Daraufhin werden Geräte, auf denen der Administrationsagent installiert ist, in der Gruppe angezeigt, die den für diese Geräte konfigurierten Verschieberegeln entspricht. Wenn Sie keine Verschieberegeln konfiguriert haben, werden die Geräte in der Gruppe **Nicht zugeordnete Geräte** angezeigt.

3 Installation des Verwaltungs-Plug-ins für Kaspersky Endpoint Security

Installieren Sie je nach verwendeter Kaspersky Security Center Verwaltungskonsole ein Verwaltungs-Plug-in für Kaspersky Endpoint Security:

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

  MMC-Plug-in für Kaspersky Endpoint Security installieren

  > Vor der Installation des MMC-basierten Verwaltungs-Plug-ins von 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:

  1. Laden Sie die Datei klcfginst.msi von der Downloadseite des Programms im Abschnitt **Kaspersky Endpoint Security für Linux** herunter (**Build → Administrations-Plug-in**).

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

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

So zeigen Sie die Liste der installierten MMC-Plug-ins für die Verwaltung 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:

   - Öffnen Sie das Kontextmenü des Knotens **Administrationsserver <Servername>** und wählen Sie den Eintrag **Eigenschaften** aus.

   - Klicken Sie im Arbeitsbereich des Knotens **Administrationsserver <Servername>** im Abschnitt **Administrationsserver** auf den Link **Eigenschaften des Administrationsservers**.

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

Wenn Sie die Kaspersky Security Center Verwaltungskonsole zur Verwaltung von Kaspersky Endpoint Security verwenden und mehrere Versionen des Programms installiert haben, müssen Sie für jede Version von Kaspersky Endpoint Security ein Verwaltungs-Plug-in 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.

- Mit dem **Web-Plug-in für die Verwaltung von Kaspersky Endpoint Security** können Sie die Anwendung 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. Die Funktionalität des Web-Plug-ins steht allen Administratoren zur Verfügung, die über einen Browser auf die Kaspersky Security Center Web Console zugreifen können.

  Web-Plug-in für Kaspersky Endpoint Security installieren

  Sie können das Web-Plug-in folgendermaßen installieren:

  - 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 Erstkonfiguration auszuführen. Sie können den Assistenten für die Erstkonfiguration auch in der Oberfläche 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 Schnellstartassistenten für Kaspersky Security Center Web Console finden Sie in der Hilfe zu Kaspersky Security Center.

  - Manuell mithilfe eines Programmpakets aus der Liste der Kaspersky-Web-Plug-ins oder aus einer Datei.

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

  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. Klicken Sie auf **Hinzufügen**.

     Dadurch wird die Liste der verfügbaren Verwaltungs-Plug-ins geöffnet. Die Liste wird automatisch aktualisiert, wenn neue Versionen der Web-Plug-ins veröffentlicht werden.

3. Wählen Sie in der Liste der verfügbaren Plug-ins das Web-Plug-in **Kaspersky Endpoint Security <Versionsnummer> für Linux** aus.

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

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

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

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

1. Laden Sie das Archiv mit dem Web-Plug-in von der Downloadseite des Programms im Abschnitt **Kaspersky Endpoint Security für Linux** herunter (**Zusätzliches Distributionspaket** → **Web Console-Plug-in**).

2. Entpacken Sie das heruntergeladene Archiv lokal.

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

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

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

5. Daraufhin wird ein Fenster geöffnet. Geben Sie in diesem Fenster den Pfad zur Datei plugin.zip und den Pfad zur Datei signature.txt an. Die Dateien befinden sich in dem Ordner, in den Sie das Archiv mit dem Web-Plug-in entpackt haben.

6. Klicken Sie auf **Hinzufügen**.

7. 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 Anwendung Kaspersky Endpoint Security vorhanden ist, werden der Endbenutzer-Lizenzvertrag und die gesamte Oberfläche in der Kaspersky Security Center Web Console in englischer Sprache angezeigt.

Video: Installation des Verwaltungs-Web-Plug-ins mithilfe des Assistenten



Video: Installation des Verwaltungs-Web-Plug-ins in isolierten Netzwerken



4 Erstellen einer Richtlinie für Kaspersky Endpoint Security

Erstellen Sie eine Richtlinie für Kaspersky Endpoint Security in Kaspersky Security Center Web Console oder in der Verwaltungskonsole (je nachdem, welche Verwaltungskonsole von Kaspersky Security Center Sie verwenden).

Konfigurieren Sie die folgenden Einstellungen abhängig davon, in welchem Modus Sie das Programm verwenden möchten:

Für den Standard-Modus

Wenn Sie im Assistenten der Verwaltungskonsole eine Richtlinie erstellt haben, geben Sie den Nutzungsmodus des Programms an: **Standard-Modus oder Endpoint Detection and Response Agent-Modus**. Wenn Sie eine Richtlinie im Assistenten von Kaspersky Security Center Web Console erstellt haben, überspringen Sie die Auswahl des Programmmodus.

Für den EDR-Agent-Modus

1. Wenn Sie im Assistenten der Verwaltungskonsole eine Richtlinie erstellt haben, geben Sie den Nutzungsmodus des Programms an: **Standard-Modus oder Endpoint Detection and Response Agent-Modus**. Wenn Sie eine Richtlinie im Assistenten von Kaspersky Security Center Web Console erstellt haben, überspringen Sie die Auswahl des Programmmodus.

2. Schließen Sie die Erstellung der Richtlinie ab, indem Sie den Anweisungen des Assistenten folgen.

3. Öffnen Sie die Eigenschaften der erstellten Richtlinie in Kaspersky Security Center Web Console oder in der Verwaltungskonsole und aktivieren Sie die Integration mit den Detection and Response-Lösungen, die Sie zum Schutz des Geräts verwenden möchten:

   - Für die Integration in Kaspersky Endpoint Detection and Response Expert (on-premises) auf der OSMP-Plattform müssen Sie die Komponente EDR Expert (on-premise) aktivieren und konfigurieren. Die Einstellungen sind in Kaspersky Security Center Web Console verfügbar

   - Für die Integration mit Kaspersky Endpoint Detection and Response auf der Kaspersky Anti Targeted Attack Platform müssen Sie die Komponente EDR Expert (on-premise) aktivieren und konfigurieren. Die Einstellungen sind in Kaspersky Security Center Web Console und in der Verwaltungskonsole verfügbar.

   - Für die Integration mit Kaspersky Network Detection and Response auf der Kaspersky Anti Targeted Attack Platform müssen Sie die Komponente NDR (KATA) aktivieren und konfigurieren. Die Einstellungen sind in Kaspersky Security Center Web Console und in der Verwaltungskonsole verfügbar.

Für den Light Agent-Modus

Im Assistenten für das Erstellen einer Richtlinie:

1. Geben Sie den **Light Agent-Modus zum Schutz virtueller Umgebungen** an.

2. Verwalten 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.

      - **Benutzerdefinierte 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 **Benutzerdefinierte Liste mit SVM-Adressen verwenden** ausgewählt haben und für den Light Agent der erweiterte Algorithmus der SVM-Auswahl verwendet wird sowie auf einer SVM der Modus zum Schutz großer Infrastrukturen aktiviert ist, dann ist die Verbindung eines Light Agents mit dieser SVM nur möglich, wenn der Standort der SVM nicht berücksichtigt wird. Im Abschnitt **Algorithmus der SVM-Auswahl** müssen Sie die Einstellung **SVM-Standort** auf **Ignorieren** setzen. Bei einem beliebigen anderen angegebenen Wert kann der Light Agent keine Verbindung zur SVM herstellen. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

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. Geben Sie bei Bedarf neue Verbindungseinstellungen an: IPv4-Adresse oder vollständig qualifizierter Domänenname (FQDN) und Port für die Verbindung mit dem Integrationsserver.

> Wenn in Ihrer Infrastruktur ein Failover-Cluster von Integrationsservern auf Linux-Basis bereitgestellt ist, müssen Sie als Adresse und Port für die Verbindung zum Integrationsserver die Adresse und den Port des Load Balancers eingeben. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

c. Wenn Sie eine manuell definierte Liste mit SVM-Adressen auswählen, erstellen Sie eine Liste der SVMs, 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 mehrere IP-Adressen oder vollständige Domänennamen der 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 Anwendung führen.

Für die übrigen Richtlinieneinstellungen können Sie die Standardwerte beibehalten. Die Standardeinstellungen bieten ein grundlegendes Schutzniveau. Nach der Installation von Kaspersky Endpoint Security können Sie die Richtlinie gemäß den Anforderungen Ihrer Organisation konfigurieren. Dazu können Sie die Szenarien zur Konfiguration von Komponenten aus dem Hilfeabschnitt Verwalten des Programms verwenden.

Video: Erstellen einer Richtlinie



5 Zentralisierte Updates von Programmdatenbanken und -modulen konfigurieren

Standardmäßig wird Kaspersky Endpoint Security ohne Antiviren-Datenbanken auf einem Gerät installiert. Das Programm wird erst funktionsfähig, nachdem die Datenbanken auf das Gerät heruntergeladen wurden. Damit der Schutz unmittelbar nach der Installation des Programms beginnt, konfigurieren Sie zentralisierte Datenbanken-Updates.

In der Kaspersky Security Center Web Console oder in der Verwaltungskonsole (je nachdem, welche Kaspersky Security Center-Verwaltungskonsole Sie verwenden):

1. Starten Sie die Aufgabe des Administrationsservers *Download von Updates in die Datenverwaltung des Administrationsservers*. Die Aufgabe wird automatisch vom Schnellstartassistenten des Administrationsservers erstellt.

   Die Aufgabe lädt das Update-Paket für Kaspersky Endpoint Security in das Update-Verzeichnis auf dem Administrationsserver herunter.

2. Erstellen Sie eine Gruppenaufgabe vom Typ *Update* für das Programm Kaspersky Endpoint Security. Geben Sie in den Aufgabeneinstellungen Folgendes an:

   - Update-Quelle: Kaspersky Security Center.
   - Zeitplan für die Aufgabe: mindestens einmal täglich. Wir empfehlen, die Aufgabe 4- bis 6-mal täglich auszuführen.

Video: Konfigurieren zentralisierter Datenbanken-Updates



6 Lizenzschlüssel hinzufügen und Aktivierungsaufgabe erstellen

Um das Programm im Standard-Modus zu aktivieren, müssen Sie dem Programm einen Lizenzschlüssel hinzufügen. Wenn einige Komponenten nicht durch Ihre Lizenz abgedeckt sind, benötigen Sie möglicherweise einen anderen Lizenzschlüssel:

Um das Programm Kaspersky Endpoint Security im EDR-Agent-Modus zu aktivieren, benötigen Sie einen Lizenzschlüssel für EDR Expert (on-premise).

Abhängig von Ihrer Infrastruktur und den Anforderungen Ihres Unternehmens können Sie eine Aktivierungsmethode auswählen:

- Wenn das Programm mit demselben Funktionsumfang auf allen Ihren Geräten installiert ist, verwenden Sie die automatische Verteilung von Lizenzschlüsseln. Der zu verteilende Lizenzschlüssel muss zunächst mithilfe einer Schlüsseldatei oder eines Aktivierungscodes zum Schlüsselspeicher von Kaspersky Security Center hinzugefügt werden. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security Center.

- Wenn sich der Funktionsumfang des Programms von Gerät zu Gerät unterscheidet, benötigen Sie unterschiedliche Lizenzschlüssel für die Aktivierung. Platzieren Sie in diesem Fall die geschützten Geräte in verschiedenen Administrationsgruppen und konfigurieren Sie eine Gruppenaufgabe zum Hinzufügen eines Schlüssels für jede Administrationsgruppe.

Kaspersky Endpoint Security im Light Agent-Modus erhält die Lizenzinformationen vom Schutzserver, nachdem die Verbindung zur SVM hergestellt wurde. Sie müssen Kaspersky Endpoint Security im Light Agent-Modus nicht separat aktivieren.

Video: Aktivierung des Programms mit einem Aktivierungscode



Video: Aktivierung des Programms mit einer Schlüsseldatei



Nachdem Sie Kaspersky Security Center vorbereitet haben, können Sie zum Bereitstellungsszenario zurückkehren und mit dem Schritt Programm installieren fortfahren.

Das Programm mithilfe von Kaspersky Security Center installieren

Besonderheiten bei der Installation:

- Der EDR Agent-Modus und der Light Agent-Modus von Kaspersky Endpoint Security werden auf Geräten mit einer Elbrus-CPU nicht unterstützt.
- Auf Arm-Geräten wird Kaspersky Endpoint Security im Light Agent-Modus nicht unterstützt.

Das empfohlene Szenario für die Installation des Programms mithilfe von Kaspersky Security Center umfasst die folgenden Schritte:

Sie können das Programm Kaspersky Endpoint Security auch über Kaspersky Security Center mithilfe des Schnellstartassistenten und des Assistenten für die Bereitstellung des Schutzes installieren.

1 Erstellung eines Installationspakets

Das Installationspaket des Programms Kaspersky Endpoint Security enthält Folgendes:

- Das Hauptprogrammpaket
- Ein Programmpaket für die Remote-Installation des Programms
- Ein Programmpaket mit der grafischen Benutzeroberfläche des Programms
- Einstellungen für die Erstkonfiguration, die während der Installation angewendet werden

Sie können ein Installationspaket auf folgende Arten erstellen:

- **Mithilfe eines Programmpakets, das auf Servern von Kaspersky gehostet wird**. In Kaspersky Security Center wird aus dem angegebenen Programmpaket automatisch ein Installationspaket erstellt.

  Video: Automatische Erstellung eines Installationspakets in Kaspersky Security Center



Um das Programm Kaspersky Endpoint Security auf Betriebssystemen mit eingeschränkter Unterstützung (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6) zu installieren, wählen Sie das mit `for legacy OS` gekennzeichnete Programmpaket aus.

- **Manuell, unter Verwendung von Dateien, die im Schritt Programmpakete vorbereiten vorbereitet wurden**. Diese Methode wird empfohlen, wenn Sie die Einstellungen für die Erstkonfiguration mithilfe einer Konfigurationsdatei festlegen möchten oder wenn Sie das erstellte Installationspaket für verschiedene Betriebssysteme oder verschiedene Paketmanager verwenden möchten.

  Video: Manuelles Erstellen eines Installationspakets in Kaspersky Security Center

  Sie können dem Installationspaket vorab heruntergeladene Datenbanken des Programms hinzufügen. Wenn Sie für die Installation ein Installationspaket mit integrierten Datenbanken verwenden, wird die Anwendung mit einsatzbereiten Datenbanken installiert und eine Aktualisierung der Datenbanken nach der Installation ist nicht erforderlich.

Ein Installationspaket kann mehrmals verwendet werden.

So bereiten Sie ein Installationspaket manuell vor

1. Entpacken Sie lokal das Archiv mit den Dateien für die Remote-Installation von Kaspersky Endpoint Security.
2. Legen Sie die Pakete mit den Hauptdateien des Programms im selben Verzeichnis ab.

   Wenn Sie das erstellte Installationspaket mit verschiedenen Betriebssystemen oder Paketmanagern verwenden möchten, legen Sie die Programmpakete für alle benötigten Typen von Betriebssystemen und Paketmanagern im Verzeichnis ab.
3. Wenn Sie die grafische Benutzeroberfläche des Programms verwenden möchten, legen Sie die Pakete für die grafische Benutzeroberfläche im selben Verzeichnis ab.

   Aktivieren Sie die Verwendung der grafischen Benutzeroberfläche, indem Sie die entsprechende Einstellung (`USE_GUI=Yes`) in den Eigenschaften des erstellten Installationspakets oder in der Konfigurationsdatei autoinstall.ini bearbeiten. Standardmäßig wird die grafische Benutzeroberfläche nicht installiert.

Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, wird die grafische Benutzeroberfläche nicht unterstützt.

4. Wenn Sie die Einstellungen für die Erstkonfiguration des Programms mithilfe einer Konfigurationsdatei festlegen möchten, öffnen Sie die Konfigurationsdatei autoinstall.ini und bearbeiten Sie sie bei Bedarf. Die Datei autoinstall.ini befindet sich in dem Ordner, in den Sie das Archiv mit den Dateien für die Remote-Installation von Kaspersky Endpoint Security entpackt haben.

   a. Standardmäßig wird die Anwendung im Standard-Modus verwendet.

   Um das Programm im EDR-Agent-Modus zu verwenden, legen Sie `ENDPOINT_AGENT_MODE=Yes` fest.

   Um das Programm im Light Agent-Modus zu verwenden, legen Sie `KSVLA_MODE=Yes` fest.

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

   b. So installieren Sie das Programm im Light Agent-Modus:

   - Wenn Sie das Programm auf einer Vorlage installieren, aus der temporäre virtuelle Maschinen erstellt werden, legen Sie `VDI_MODE=Yes` fest. Diese Einstellung aktiviert den Modus zum Schutz der VDI-Infrastruktur, um die Leistung des Programms auf temporären virtuellen Maschinen zu optimieren.

   - Geben Sie die Rolle der virtuellen Maschinen, die Sie schützen möchten, in der virtuellen Infrastruktur (Server oder Workstation) an (`SERVER_MODE=Yes|No`). 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.

   Sie können die Erstkonfiguration des Programms auch später in den Eigenschaften des erstellten Installationspakets auf der Registerkarte **Einstellungen** ändern.

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 in der Web Console:

1. Wählen Sie im Hauptfenster der Web Console einen der folgenden Abschnitte aus:

   - **Gerätesuche 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.

3. Wenn Sie die Web Console verwenden, wählen Sie aus, wie Sie ein Installationspaket erstellen möchten:

   - **Installationspaket aus einer Datei erstellen**. Das Installationspaket wird aus der Archivdatei erstellt, die Sie zuvor vorbereitet haben.

   - **Installationspaket für eine Kaspersky-Anwendung erstellen**. Das Installationspaket wird aus einem Programmpaket erstellt, das auf den Servern von Kaspersky gehostet wird.

   Wenn Sie Kaspersky Security Center Cloud Console verwenden, wird das Installationspaket aus dem Programmpaket erstellt, das auf Kaspersky-Servern gehostet wird.

4. Je nach Methode zum Erstellen des Pakets:

   - Geben Sie den Paketnamen an, klicken Sie auf die Schaltfläche **Durchsuchen** und geben Sie den Pfad zu dem Archiv an, das Sie zum Erstellen des Installationspakets vorbereitet haben.

   - Wählen Sie das Programmpaket für Kaspersky Endpoint Security aus. Lesen Sie im rechten Fenster die Informationen zum Programmpaket und klicken Sie auf die Schaltfläche **Herunterladen und Installationspaket erstellen**. Der Vorgang zur Erstellung des Installationspakets wird gestartet.

5. 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.

6. Schließen Sie den Assistenten ab.

   Das Installationspaket wird erstellt und der Liste mit Installationspaketen hinzugefügt.

7. Öffnen Sie die Eigenschaften des Installationspakets und wechseln Sie zur Registerkarte **Einstellungen**.

   - Wenn Sie das Programm im EDR-Agent-Modus installieren, wählen Sie für die Einstellung **Verwendungsmodus** die Option **Endpoint Detection and Response Agent** aus.

   - Wenn Sie das Programm im Light Agent-Modus installieren, geben Sie die folgenden Einstellungen an:

     Wählen Sie unter **Verwendungsmodus** die Option **Light Agent für den Schutz virtueller Umgebungen** aus.

     VDI-Schutzmodus aktivieren. Aktivieren Sie das Kontrollkästchen, um den Modus zum Schutz der VDI-Infrastruktur zu aktivieren. Dies wird empfohlen, wenn die Anwendung auf einer Vorlage für virtuelle Maschinen installiert wird, aus der temporäre virtuelle Maschinen erstellt werden. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

     Die geschützte virtuelle Maschine wird als Server verwendet. Die Rolle der virtuellen Maschine, auf der die Anwendung installiert wird: Server oder Workstation. Das Kontrollkästchen ist standardmäßig aktiviert (die VM wird in der virtuellen Infrastruktur als Server verwendet).

   - Verwalten Sie bei Bedarf weitere Einstellungen der Erstkonfiguration.

     Eine Beschreibung aller Einstellungen der Erstkonfiguration des Programms im Installationspaket finden Sie unter Anhang 1.

So erstellen Sie ein Installationspaket in der Verwaltungskonsole:

So erstellen Sie ein Installationspaket mithilfe vorbereiteter Dateien:

1. Wählen Sie in der Konsolenstruktur den Punkt **Erweitert** → **Remote-Installation** → **Installationspakete** aus.

2. Klicken Sie auf **Installationspaket erstellen**.

   Der Assistent für neue Pakete wird gestartet.

3. Klicken Sie auf die Schaltfläche **Installationspaket für eine Kaspersky-Anwendung erstellen**.

4. Geben Sie den Namen des neuen Installationspakets ein und wechseln Sie zum nächsten Schritt des Assistenten.

5. Geben Sie den Pfad zur Datei kesl.kud an. Die Datei befindet sich in dem Ordner, in den Sie das Archiv mit den Dateien zur Installation des Programms (kesl.zip) im Schritt Programmpakete vorbereiten entpackt haben.

   Im Fenster wird der Name und die Version der Anwendung angezeigt. Wechseln Sie zum nächsten Schritt des Assistenten.

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 fortzufahren, bestätigen Sie, dass Sie die vollständigen Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie gelesen haben und akzeptieren. Aktivieren Sie im nächsten Fenster beide Kontrollkästchen, um zu bestätigen.

   Wechseln Sie zum nächsten Schritt des Assistenten.

7. Der Assistent lädt die Dateien, die für die Installation der Anwendung erforderlich sind, auf den Administrationsserver von Kaspersky Security Center herunter. Warten Sie, bis der Download abgeschlossen ist, und schließen Sie den Assistenten ab.

8. Öffnen Sie die Eigenschaften des Installationspakets und wechseln Sie zur Registerkarte **Anwendungseinstellungen**.

   - Wenn Sie das Programm im EDR-Agent-Modus installieren, wählen Sie für die Einstellung **Ausführungsmodus der Anwendung** die Option **Endpoint Detection and Response Agent** aus.

   - Wenn Sie das Programm im Light Agent-Modus installieren, geben Sie die folgenden Einstellungen an:

     Ausführungsmodus der Anwendung. Wählen Sie die Option **Light Agent zum Schutz virtueller Umgebungen** aus.

     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 Anwendung auf einer Vorlage für virtuelle Maschinen installiert wird, aus der temporäre virtuelle Maschinen erstellt werden. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

     Die geschützte virtuelle Maschine wird als Server verwendet. Die Rolle der virtuellen Maschine, auf der die Anwendung installiert wird: Server oder Workstation. Dieses Kontrollkästchen ist standardmäßig aktiviert.

     Im Light Agent-Modus nicht verfügbar:

     - Update-Quellen für die Programmdatenbanken konfigurieren und Update starten
     - Allgemeine Proxy-Server-Einstellungen anpassen
     - App aktivieren

     Das Programm im Light Agent-Modus erhält nach dem Verbinden mit der SVM Datenbanken-Updates und Lizenzinformationen vom Schutzserver. Sie müssen Kaspersky Endpoint Security nicht separat aktivieren oder Datenbanken-Updates konfigurieren.

   - Verwalten Sie bei Bedarf weitere Einstellungen der Erstkonfiguration.

     Eine Beschreibung aller Einstellungen der Erstkonfiguration des Programms im Installationspaket finden Sie unter Anhang 1.

   Sie können die Erstkonfiguration des Programms später in den Eigenschaften des erstellten Installationspakets im Abschnitt **Anwendungseinstellungen** durchführen.

Der Assistent erstellt auf Grundlage des Programmpakets von den Kaspersky-Servern ein Installationspaket.

1. Wählen Sie in der Konsolenstruktur den Punkt **Erweitert → Remote-Installation → Installationspakete** aus.

2. Klicken Sie auf die Schaltfläche **Zusätzliche Aktionen → Aktuelle Versionen von Kaspersky-Programmen anzeigen**.

3. Wählen Sie in der Liste das Programmpaket für Kaspersky Endpoint Security aus und klicken Sie auf die Schaltfläche **Installationspaket herunterladen und erstellen**.

4. 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 fortzufahren, bestätigen Sie, dass Sie die vollständigen Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie gelesen haben und akzeptieren. Aktivieren Sie zur Bestätigung beide Kontrollkästchen im Bestätigungsfenster und klicken Sie auf die Schaltfläche **Alle akzeptieren**.

5. Warten Sie, bis die Installation abgeschlossen ist. Das Installationspaket wird erstellt und der Liste mit Installationspaketen hinzugefügt.

6. Öffnen Sie die Eigenschaften des Installationspakets und wechseln Sie zum Abschnitt **Anwendungseinstellungen**.

   - Wenn Sie das Programm im EDR-Agent-Modus installieren, wählen Sie für die Einstellung **Ausführungsmodus der Anwendung** die Option **Endpoint Detection and Response Agent** aus.

   - Wenn Sie das Programm im Light Agent-Modus installieren, geben Sie die folgenden Einstellungen an:

     Ausführungsmodus der Anwendung. Wählen Sie die Option **Light Agent zum Schutz virtueller Umgebungen** aus.

     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 Anwendung auf einer Vorlage für virtuelle Maschinen installiert wird, aus der temporäre virtuelle Maschinen erstellt werden. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

     Die geschützte virtuelle Maschine wird als Server verwendet. Die Rolle der virtuellen Maschine, auf der die Anwendung installiert wird: Server oder Workstation. Dieses Kontrollkästchen ist standardmäßig aktiviert.

     Die folgenden Einstellungen sind im Light Agent-Modus nicht verfügbar:

     - Update-Quellen für die Programmdatenbanken konfigurieren und Update starten
     - Allgemeine Proxy-Server-Einstellungen anpassen
     - App aktivieren

     Das Programm im Light Agent-Modus erhält nach dem Verbinden mit der SVM Datenbanken-Updates und Lizenzinformationen vom Schutzserver. Sie müssen Kaspersky Endpoint Security nicht separat aktivieren oder Datenbanken-Updates konfigurieren.

   - Verwalten Sie bei Bedarf weitere Einstellungen der Erstkonfiguration.

     Eine Beschreibung aller Einstellungen der Erstkonfiguration des Programms im Installationspaket finden Sie unter Anhang 1.

   Sie können die Erstkonfiguration des Programms später in den Eigenschaften des erstellten Installationspakets im Abschnitt **Anwendungseinstellungen** durchführen.

2 Installieren des Programms auf Geräten im Unternehmensnetzwerk

Sie können das Programm über Kaspersky Security Center mithilfe der Aufgabe zur Remote-Installation von Programmen installieren.

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

Die Erstkonfiguration des Programms erfolgt automatisch gemäß den Einstellungen, die in den Eigenschaften des Installationspakets oder in der Konfigurationsdatei im Installationspaket festgelegt sind.

Video: Installation, Update der Datenbanken und Überprüfung der Funktionsfähigkeit von Kaspersky Endpoint Security



3 Datenbanken-Update des Programms

Wenn Sie das Programm im Standard-Modus oder im EDR Agent-Modus installiert haben, führen Sie in der Web Console oder in der Verwaltungskonsole (je nachdem, welche Verwaltungskonsole von Kaspersky Security Center Sie verwenden) die Gruppenaufgabe *Update* aus, die im Schritt „Zentralisierte Updates von Programmdatenbanken und -modulen konfigurieren“ erstellt wurde. Weitere Informationen zum Update der Datenbanken von Kaspersky Endpoint Security finden Sie im Abschnitt Update der Programmdatenbanken und -module.

Wenn beim ersten Update der Datenbanken und Module innerhalb von 24 Stunden nach der Installation des Programms kritische Updates empfangen werden, wird das Programm automatisch neu gestartet.

4 Überprüfung der Programmgesundheit

Dadurch wurde das Programm Kaspersky Endpoint Security installiert und aktiviert, und die Programmdatenbanken wurden aktualisiert. Nach der Installation wird das Programm automatisch gestartet. Standardmäßig sind die folgenden Komponenten aktiviert:

- 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.

Stellen Sie sicher, dass das Programm einsatzbereit ist.

Überprüfen des Schutzstatus eines Geräts in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Asset-Management** → **Assets (Geräte)** aus.

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Um eine verschachtelte Gruppe auszuwählen, klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Hierarchie anzeigen**.

   In der Liste werden nur die verwalteten Geräte der ausgewählten Administrationsgruppe angezeigt.

3. Klicken Sie auf den Namen eines Geräts.

   Dadurch wird das Eigenschaftenfenster für das verwaltete Gerät geöffnet.

4. Wählen Sie auf die Registerkarte **Allgemein** den Abschnitt **Schutz**. Im Feld **Gerätestatus** sollte *OK* angezeigt werden.

   Wenn im Feld **Gerätestatus** Informationen zu unzureichenden Berechtigungen für Systemverzeichnisse angezeigt werden, überprüfen Sie lokal auf diesem Gerät die Berechtigungen für die folgenden Verzeichnisse: /var/opt/kaspersky, /var/log/kaspersky und /opt/kaspersky. Stellen Sie sicher, dass der Besitzer root ist und nur der Besitzer Schreibzugriff auf diese Verzeichnisse hat.

5. Wechseln Sie zur Registerkarte **Programme**.

6. Klicken Sie in der Liste der auf dem Gerät installierten Anwendungen auf den Namen der Anwendung Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der App wird geöffnet.

7. Sehen Sie auf der Registerkarte **Allgemein** im Abschnitt **Informationen** unter **Programmdatenbanken** nach. Stellen Sie sicher, dass die Programmdatenbanken auf dem neuesten Stand sind.

8. Wechseln Sie auf der Registerkarte **Allgemein** zum Abschnitt **Lizenzen** und stellen Sie sicher, dass das Programm aktiviert ist.

9. Wenn Sie das Programm im EDR Agent-Modus installiert haben, wechseln Sie auf der Registerkarte **Allgemein** zum Abschnitt **Komponenten** und stellen Sie sicher, dass die Integrationen, die Sie im Schritt „Richtlinie für Kaspersky Endpoint Security erstellen“ konfiguriert haben, den Status *Wird ausgeführt* haben.

10. Wenn Sie das Programm im Light Agent-Modus installiert haben, wechseln Sie auf der Registerkarte **Allgemein** zum Abschnitt **Komponenten** und stellen Sie sicher, dass in der Zeile **Light Agent-Modus zum Schutz virtueller Umgebungen** der Status *Wird ausgeführt* angezeigt wird. Das bedeutet, dass das Programm im Light Agent-Modus verwendet wird.

Überprüfen des Schutzstatus eines Geräts in der Verwaltungskonsole

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.

   Dadurch wird das Eigenschaftenfenster für das verwaltete Gerät geöffnet.

4. Wählen Sie den Abschnitt **Schutz** aus. Im Feld **Gerätestatus** sollte *OK/Sichtbar im Netzwerk* angezeigt werden.

   Wenn im Feld **Gerätestatus** Informationen zu unzureichenden Berechtigungen für Systemverzeichnisse angezeigt werden, überprüfen Sie lokal auf diesem Gerät die Berechtigungen für die folgenden Verzeichnisse: /var/opt/kaspersky, /var/log/kaspersky und /opt/kaspersky. Stellen Sie sicher, dass der Besitzer root ist und nur der Besitzer Schreibzugriff auf diese Verzeichnisse hat.

5. Wechseln Sie zum Abschnitt **Programme**.

6. Wählen Sie in der Liste der auf dem Gerät installierten Programme das Programm Kaspersky Endpoint Security aus und öffnen Sie durch Doppelklick das Eigenschaftenfenster des Programms.

7. Sehen Sie im Abschnitt **Allgemein** im Feld **Programmdatenbanken** nach. Stellen Sie sicher, dass die Programmdatenbanken auf dem neuesten Stand sind.

8. Wechseln Sie zum Abschnitt **Lizenzschlüssel** und stellen Sie sicher, dass das Programm aktiviert ist.

9. Wenn Sie das Programm im EDR Agent-Modus installiert haben, wechseln Sie zum Abschnitt **Komponenten** und stellen Sie sicher, dass die Integrationen, die Sie im Schritt „Richtlinie für Kaspersky Endpoint Security erstellen“ konfiguriert haben, den Status *Wird ausgeführt* haben.

10. Wenn Sie das Programm im Light Agent-Modus installiert haben, wechseln Sie zum Abschnitt **Komponenten** und stellen Sie sicher, dass in der Zeile **Light Agent-Modus zum Schutz virtueller Umgebungen** der Status *Wird ausgeführt* angezeigt wird. Das bedeutet, dass das Programm im Light Agent-Modus verwendet wird.

Nützliche Artikel

Vorgehensweise, wenn Aufgaben nicht ausgeführt oder Richtlinien nicht angewendet werden

Vorgehensweise, wenn das Gerät den folgenden Status aufweist: „Ungültige Richtlinieneinstellungen. Richtlinie wurde nicht angewendet.“

Fehler: „Die App wird von der aktuellen Version von Kaspersky Security Center Web Console nicht unterstützt oder das Web-Plug-in der App ist nicht installiert“

Beheben eines Problems bei der Installation der grafischen Benutzeroberfläche

Beschreibung der Installationsfehlercodes

Fehler nach der Installation von Kaspersky Endpoint Security

Nachdem Sie Kaspersky Endpoint Security installiert haben, können Sie zum Bereitstellungsszenario zurückkehren und mit dem Schritt Zusätzliche Konfigurationsschritte nach der Installation unter bestimmten Betriebssystemen fortfahren.

Anwendung über die Befehlszeile installieren

Besonderheiten bei der Installation:

- Der EDR Agent-Modus und der Light Agent-Modus von Kaspersky Endpoint Security werden auf Geräten mit einer Elbrus-CPU nicht unterstützt.
- Auf Arm-Geräten wird Kaspersky Endpoint Security im Light Agent-Modus nicht unterstützt.
- Sie benötigen Root-Rechte, um das Programm und die grafische Benutzeroberfläche zu installieren.
- Der Assistent zur Erstkonfiguration muss mit Root-Rechten ausgeführt werden.
- Wenn die Version des apt-Paketmanagers älter ist als 1.1.X, muss je nach Betriebssystem der dpkg-Paketmanager für die Installation verwendet werden.

Das empfohlene Szenario für die Installation des Programms über die Befehlszeile umfasst die folgenden Schritte:

1 Installation der Kaspersky Endpoint Security -Anwendung

Bevor Sie mit der Installation beginnen, legen Sie das heruntergeladene Paket mit den Hauptdateien des Programms im Verzeichnis /tmp auf dem Gerät ab.

So installieren Sie das Programm aus einem RPM-Paket

Auf einem 32-Bit-Betriebssystem

```
yum install kesl-12.5.0-<build number>.i386.rpm
```

Auf einem 64-Bit-Betriebssystem

```
yum install kesl-12.5.0-<build number>.x86_64.rpm
```

Auf einem 64-Bit-ALT-Betriebssystem

```
apt-get install kesl-12.5.0-<build number>.x86_64.rpm
```

Auf einem 64-Bit-Betriebssystem für die Arm-Architektur

```
yum install kesl-12.5.0-<build number>.aarch64.rpm
```

Auf einem 64-Bit-ALT-Betriebssystem für die Arm-Architektur

```
apt-get install kesl-12.5.0-<build number>.aarch64.rpm
```

Auf einem 64-Bit-Betriebssystem für die Elbrus-Architektur

```
yum install kesl-12.5.0-<build number>.2ek.rpm
```

Auf einem 64-Bit-ALT-Betriebssystem für die Elbrus-Architektur

```
apt-get install kesl-12.5.0-<build number>.2ek.rpm
```

Auf einem 64-Bit-Betriebssystem mit eingeschränkter Unterstützung (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6)

```
rpm -i kesl-12.5.0-<build number>.x86_64.rpm
```

Um das Programm unter CentOS 5.2, CentOS 5.4, CentOS 6.4 oder CentOS 6.6 zu installieren, müssen Sie das mit OLD gekennzeichnete Distributionspaket von der Website herunterladen.

So installieren Sie das Programm aus einem DEB-Paket

Auf einem 32-Bit-Betriebssystem

```
apt-get install ./kesl_12.5.0-<build number>_i386.deb
```

Auf einem 64-Bit-Betriebssystem

```
apt-get install ./kesl_12.5.0-<build number>_amd64.deb
```

Auf einem 64-Bit-Betriebssystem für die Arm-Architektur

```
apt-get install ./kesl_12.5.0-<build number>_arm64.deb
```

Auf einem 64-Bit-Betriebssystem für die Elbrus-Architektur

```
apt-get install ./kesl_12.5.0-<build number>_2ek.deb
```

2 Installation der grafischen Benutzeroberfläche der Anwendung

Wenn Sie das Programm über die grafische Benutzeroberfläche verwalten möchten, müssen Sie die grafische Benutzeroberfläche auf demselben Gerät wie das Programm installieren.

Besonderheiten der grafischen Benutzeroberfläche des Programms:

- Sie können die grafische Benutzeroberfläche nicht auf einem Gerät installieren, auf dem das Programm Kaspersky Endpoint Security nicht installiert ist.
- Wenn das Programm im Light Agent-Modus verwendet wird, wird die grafische Benutzeroberfläche nicht unterstützt.

Bevor Sie mit der Installation beginnen, legen Sie das heruntergeladene Paket mit den Dateien der grafischen Benutzeroberfläche des Programms im Verzeichnis /tmp auf dem Gerät ab.

So installieren Sie die grafische Benutzeroberfläche des Programms aus einem RPM-Paket

Auf einem 32-Bit-Betriebssystem

```
yum install kesl-gui-12.5.0-<build number>.i386.rpm
```

Auf einem 64-Bit-Betriebssystem

```
yum install kesl-gui-12.5.0-<build number>.x86_64.rpm
```

Auf einem 64-Bit-ALT-Betriebssystem

```
apt-get install kesl-gui-12.5.0-<build number>.x86_64.rpm
```

Auf einem 64-Bit-Betriebssystem für die Arm-Architektur

```
yum install kesl-gui-12.5.0-<build number>.aarch64.rpm
```

Auf einem 64-Bit-ALT-Betriebssystem für die Arm-Architektur

```
apt-get install kesl-gui-12.5.0-<build number>.aarch64.rpm
```

Auf einem 64-Bit-Betriebssystem auf der Elbrus-Architektur

```
yum install kesl-gui-12.5.0-<build number>.2ek.rpm
```

Auf einem 64-Bit-ALT-Betriebssystem auf der Elbrus-Architektur

```
apt-get install kesl-gui-12.5.0-<build number>.2ek.rpm
```

Auf einem 64-Bit-Betriebssystem mit eingeschränkter Unterstützung (CentOS 6.4, CentOS 6.6)

```
rpm -i kesl-gui-12.5.0-<build number>.x86_64.rpm
```

Um das Programm unter CentOS 6.4 oder CentOS 6.6 zu installieren, müssen Sie das mit `OLD` gekennzeichnete Distributionspaket von der Website herunterladen.

So installieren Sie die grafische Benutzeroberfläche des Programms aus einem DEB-Paket

Auf einem 32-Bit-Betriebssystem

```
apt-get install ./kesl-gui_12.5.0-<build number>_i386.deb
```

Auf einem 64-Bit-Betriebssystem

```
apt-get install ./kesl-gui_12.5.0-<build number>_amd64.deb
```

Auf einem 64-Bit-Betriebssystem für die Arm-Architektur

```
apt-get install ./kesl-gui_12.5.0-<build number>_arm64.deb
```

Auf einem 64-Bit-Betriebssystem für die Elbrus-Architektur

```
apt-get install ./kesl-gui_12.5.0-<build number>_2ek.deb
```

3 Erstkonfiguration der App

Die Erstkonfiguration ist erforderlich, um die Anwendung auf ihre Ausführung vorzubereiten und den Schutz für das Client-Gerät zu aktivieren.

Wenn auf dem Gerät die Erstkonfiguration der Anwendung nicht ausgeführt wurde, können Sie auf dem Gerät die Anwendung weder verwenden noch deren Version aktualisieren.

Die Ersteinrichtung des Programms erfolgt mithilfe des Assistenten für die Ersteinrichtung aus dem Distributionskit von Kaspersky Endpoint Security. Sie können die Ersteinrichtung im interaktiven Modus oder im automatischen Modus durchführen.

So führen Sie die Ersteinrichtung des Programms interaktiv durch.

Schritt 1. Starten des Assistenten

Starten Sie den Assistenten für die Ersteinrichtung.

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

Geben Sie nach Aufforderung des Assistenten Schritt für Schritt die Werte der Einstellungen für die Ersteinrichtung von Kaspersky Endpoint Security an.

Wenn der Administrationsagent auf dem Gerät installiert ist und Sie das Programm im Standard-Modus oder im EDR Agent-Modus installieren, können Sie die Schritte des Assistenten für die Ersteinrichtung überspringen, die sich auf das Aktualisieren der Programmdatenbanken und das Aktivieren des Programms beziehen.

Schritt 2. Auswählen des Standard-Modus oder des Light Agent-Modus

Geben Sie `yes` ein, um das Programm im Light Agent-Modus zu verwenden.

Geben Sie `no` ein, um das Programm im Standard-Modus zu verwenden.

Wenn Sie das Programm im EDR Agent-Modus verwenden möchten, müssen Sie in diesem Schritt `no` eingeben und im nächsten Schritt den EDR Agent-Modus auswählen.

Nachdem die Erstkonfiguration abgeschlossen ist, können Sie den Nutzungsmodus der Anwendung nicht mehr ändern.

Schritt 3. Auswählen des Modus: Standard oder Endpoint Detection and Response Agent

Dieser Schritt wird angezeigt, wenn Sie sich in Schritt 2 dafür entschieden haben, das Programm im Standard-Modus zu verwenden.

Geben Sie `yes` ein, um das Programm im EDR Agent-Modus zu verwenden.

Geben Sie `no` ein, um das Programm im Standard-Modus zu verwenden.

Nachdem die Erstkonfiguration abgeschlossen ist, können Sie den Nutzungsmodus der Anwendung nicht mehr ändern.

Schritt 4. Integration mit Kaspersky Endpoint Detection and Response Expert (cloud)

Dieser Schritt wird angezeigt, wenn Sie sich in Schritt 3 dafür entschieden haben, das Programm im Standard-Modus zu verwenden.

Geben Sie `yes` ein, um die Integration mit Kaspersky Endpoint Detection and Response Expert (cloud) zu verwenden.

Geben Sie `no` ein, um die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) zu verwenden.

Schritt 5. Auswählen der Rolle der virtuellen Maschine

Dieser Schritt wird angezeigt, wenn Sie sich in Schritt 2 dafür entschieden haben, das Programm im Light Agent-Modus zu verwenden.

Geben Sie 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.

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.

Schritt 6. Aktivieren des Modus zum Schutz der VDI-Infrastruktur

Dieser Schritt wird angezeigt, wenn Sie sich in Schritt 2 dafür entschieden haben, das Programm im Light Agent-Modus zu verwenden.

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 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.

Schritt 7. Zeichensatz auswählen

In diesem Schritt zeigt der Assistent die Liste der unterstützten Gebietsschemas im RFC 3066-Format an.

Geben Sie ein Gebietsschema so an, wie es hier aufgeführt ist. Dieser Standard wird verwendet, um:

- die Texte des Endbenutzer-Lizenzvertrags, der Datenschutzrichtlinie und der Erklärung zu Kaspersky Security Network zu lokalisieren, die während der Erstinstallation angezeigt werden.
- die Ereignisse der Anwendung zu lokalisieren, die an Kaspersky Security Center übertragen werden.

Zur Darstellung der grafischen Oberfläche und der Befehlszeile der Anwendung wird die Lokalisierung verwendet, die in der Umgebungsvariablen `LANG` angegeben ist. Wenn die angegebene Lokalisierung von der Anwendung nicht unterstützt wird, verwendet die Anwendung die englische Lokalisierung.

Schritt 8. Anzeigen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie

Lesen Sie in diesem Schritt den Endbenutzer-Lizenzvertrag, der zwischen Ihnen und Kaspersky geschlossen wird, sowie die Datenschutzrichtlinie, die die Verarbeitung und Übermittlung von Daten beschreibt.

Schritt 9. Endbenutzer-Lizenzvertrag akzeptieren

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

- `yes` (oder `y`), wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren.
- `no` (oder `n`), wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags nicht akzeptieren.

Wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags nicht akzeptieren, wird der Konfigurationsprozess von Kaspersky Endpoint Security abgebrochen.

Schritt 10. Annahme der Datenschutzrichtlinie

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

- `yes` (oder `y`), wenn Sie die Bedingungen der Datenschutzrichtlinie akzeptieren.
- `no` (oder `n`), wenn Sie die Bedingungen der Datenschutzrichtlinie nicht akzeptieren.

Wenn Sie die Bedingungen der Datenschutzrichtlinie nicht akzeptieren, wird der Konfigurationsprozess von Kaspersky Endpoint Security abgebrochen.

Schritt 11. Verwenden von Kaspersky Security Network

Akzeptieren Sie in diesem Schritt die Nutzungsbedingungen von Kaspersky Security Network oder lehnen Sie sie ab:

- Geben Sie `yes` (oder `y`) ein, wenn Sie die Bedingungen der Erklärung zu Kaspersky Security Network akzeptieren. Der erweiterte KSN-Modus wird aktiviert.
- Geben Sie `no` (oder `n`) ein, wenn Sie die Bedingungen der Erklärung zu Kaspersky Security Network nicht akzeptieren.

Die Datei "ksn_licence.<Sprach-ID>", die den Text der Erklärung zu Kaspersky Security Network enthält, befindet sich im Verzeichnis opt/kaspersky/kesl/doc/.

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 Security Network aktiviert ist, wird automatisch der Cloud-Modus aktiviert, in dem Kaspersky Endpoint Security die schlanke Version der Malware-Datenbanken verwendet.

Schritt 12. Benutzer aus privilegierten Gruppen entfernen

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

Geben Sie an, ob 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 Anwendung.

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 Anwendung die Benutzer aus den privilegierten Gruppen entfernt.

Schritt 13. Einem Benutzer die Administratorrolle zuweisen

In diesem Schritt fordert Sie der Assistent auf, die Rolle des Administrators (admin) zuzuweisen.

Geben Sie den Namen des Benutzers ein, dem Sie die Administratorrolle zuweisen möchten. Mit der Administratorrolle können Sie ohne Verwendung des Befehls `sudo` die Anwendungs- und Aufgabeneinstellungen über die grafische Oberfläche und die Befehlszeile der Anwendung verwalten.

Sie können einem Benutzer die Administratorrolle später nach Abschluss der Erstkonfiguration zuweisen.

Schritt 14. Konfigurieren des Mechanismus zum Abfangen von Systemereignissen

Das Programm kann den Mechanismus zum Abfangen von Systemereignissen verwenden, der auf dem aktualisierbaren Kernel-Modul basiert, wenn das Betriebssystem die Anforderungen für die Installation dieses Moduls erfüllt. Wenn das Betriebssystem diese Anforderungen nicht erfüllt, aber die fanotify-Technologie unterstützt, verwendet das Programm fanotify zum Abfangen von Systemereignissen. Wenn das Betriebssystem die fanotify-Technologie nicht unterstützt, kompiliert und verwendet das Programm ein spezielles Kernel-Modul, um Systemereignisse für den Schutz vor bedrohlichen Dateien abzufangen. Wenn alle erforderlichen Pakete installiert sind, wird die Kompilierung des Kernel-Moduls beim Start des Schutzes vor bedrohlichen Dateien automatisch gestartet. Wenn die notwendigen Pakete nicht auf dem Gerät gefunden werden, fordert Kaspersky Endpoint Security Sie auf, diese zu installieren. Wenn das Herunterladen der Pakete fehlschlägt, wird eine Fehlermeldung ausgegeben.

- Geben Sie `yes` ein, wenn Sie den Abfangmechanismus auf Basis des aktualisierbaren Kernel-Moduls verwenden möchten.
- Geben Sie `no` ein, wenn Sie den Abfangmechanismus auf Basis der fanotify-Technologie verwenden möchten.

Wenn Sie den Abfangmechanismus basierend auf dem aktualisierbaren Kernel-Modul auswählen, geben Sie die folgenden Parameter an:

- Die von der Anwendung ausführte Aktion, wenn das aktualisierbare Kernel-Modul nicht gestartet werden kann:
  - Geben Sie `yes` ein, wenn die Anwendung nach einem fehlgeschlagenen Start des aktualisierbaren Kernel-Moduls zur Verwendung der fanotify-Technologie zum Abfangen von Dateiereignissen übergehen soll.
  - Geben Sie `no` ein, wenn die Anwendung nach einem fehlgeschlagenen Start des aktualisierbaren Kernel-Moduls das Abfangen von Dateiereignissen einstellen soll.

    Wenn das Abfangen von Systemereignissen von der Anwendung nicht verwendet wird, findet keine Dateiuntersuchung in Echtzeit statt. Dies reduziert die Schutzstufe des Geräts.

- Modus des Anwendungsneustarts beim Übergang zur Verwendung des aktualisierbaren Kernel-Moduls. Um das Modul zu starten, muss die Anwendung entweder automatisch oder manuell neu gestartet werden:

  Es wird empfohlen, die Anwendung beim Übergang zur Verwendung des aktualisierbaren Kernel-Moduls automatisch neuzustarten. Nach einem manuellen Neustart kann der Start des aktualisierbaren Kernel-Moduls zu Ausführungsfehlern der Anwendung führen.

Geben Sie `yes` ein, um den automatischen Neustart der Anwendung für den Start des Moduls zu erlauben.

Schritt 15. Automatische Konfiguration von SELinux aktivieren

Dieser Schritt wird angezeigt, wenn das Zugriffskontrollsystem SELinux in Ihrem Betriebssystem installiert ist.

Geben Sie `yes` ein, um SELinux automatisch für die Arbeit mit Kaspersky Endpoint Security zu konfigurieren. Wenn das Programm die automatische Konfiguration von SELinux nicht ausführen kann (beispielsweise, wenn das Dienstprogramm semanage fehlt), zeigt der Assistent eine Fehlermeldung an und fordert den Benutzer auf, SELinux manuell zu konfigurieren.

Geben Sie `no` ein, wenn Sie die automatische Konfiguration des SELinux-Systems nicht ausführen möchten.

Standardmäßig schlägt der Assistent `yes` vor.

Falls erforderlich, können Sie SELinux später nach Abschluss der Erstkonfiguration des Programms manuell für die Arbeit mit dem Programm konfigurieren.

Schritt 16. Update-Quelle konfigurieren

Dieser Schritt wird angezeigt, wenn Sie Kaspersky Endpoint Security im Standard-Modus oder im EDR-Agent-Modus installieren.

Geben Sie die Update-Quelle für Datenbanken und Programm-Module an. Die Anwendungsdatenbanken enthalten Beschreibungen der Signaturen von Bedrohungen und der Methoden zu ihrer Bekämpfung. Die Anwendung verwendet diese Einträge bei der Suche und der Neutralisierung von Bedrohungen. Die Virenanalysten von Kaspersky fügen regelmäßig Einträge über Bedrohungen hinzu.

Geben Sie einen der folgenden Werte ein:

- `KLServers` – Die Anwendung erhält die Updates von einem der Kaspersky-Update-Server.
- `SCServer` – Die Anwendung lädt die Updates von einem in Ihrer Organisation installierten Administrationsserver für Kaspersky Security Center auf das geschützte Gerät herunter. Sie können diese Update-Quelle auswählen, wenn Sie Kaspersky Security Center für die zentrale Verwaltung des Schutzes der Geräte in Ihren Unternehmen benutzen.
- `Custom` – Die Anwendung lädt Updates aus einer benutzerdefinierten Quelle herunter. Sie können die Adresse einer benutzerdefinierten Update-Quelle als lokales Verzeichnis (beispielsweise /home/databases) oder als entfernten HTTP- oder HTTPS-Server (beispielsweise http://example.com/databases/) angeben.

Schritt 17. Proxyserver-Einstellungen

Dieser Schritt wird angezeigt, wenn Sie Kaspersky Endpoint Security im Standard-Modus oder im EDR-Agent-Modus installieren.

Wenn Sie für Ihre Internetverbindung einen Proxyserver verwenden, geben Sie die Adresse Ihres Proxyservers in einem der folgenden Formate ein:

- `[<connection protocol>://]<address of proxy server>:<port>`, wenn für die Verbindung mit dem Proxyserver keine Authentifizierung erforderlich ist;
- `[<connection protocol>://][<user name>:<password>@]<address of proxy server>:<port>`, wenn für die Verbindung mit dem Proxyserver eine Authentifizierung erforderlich ist. Geben Sie eine IPv6-Adresse in eckigen Klammern ein.

  Das Herstellen einer Verbindung mit dem Proxyserver über das HTTPS-Protokoll wird nicht unterstützt. 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 verwendet eine unsichere Verbindung und das Benutzerkonto ist möglicherweise kompromittiert.

Wenn Sie keinen Proxyserver verwenden, geben Sie `no` ein.

Standardmäßig schlägt die Anwendung den Wert `no` vor.

Sie können den Proxyserver später konfigurieren, nachdem Sie die Ersteinrichtung der Anwendung abgeschlossen haben.

Schritt 18. Update der Anwendungsdatenbanken starten

Dieser Schritt wird angezeigt, wenn Sie Kaspersky Endpoint Security im Standard-Modus oder im EDR-Agent-Modus installieren.

In diesem Schritt bietet der Assistent an, die Aufgabe zum Datenbanken-Update auf dem Client-Gerät sofort nach der Installation auszuführen.

Wenn Sie auf das Starten des Updates der Anwendungsdatenbanken verzichten möchten, geben Sie `no` ein.

Standardmäßig schlägt der Assistent `yes` vor.

Die Anwendung Kaspersky Endpoint Security kann den vollständigen Schutz des Geräts erst nach dem Update der Anwendungsdatenbanken sicherstellen.

Sie können die Update-Aufgabe später starten, nachdem Sie die Ersteinrichtung der Anwendung abgeschlossen haben.

Schritt 19. Automatische Updates für die Anwendungsdatenbanken aktivieren

Dieser Schritt wird angezeigt, wenn Sie Kaspersky Endpoint Security im Standard-Modus oder im EDR-Agent-Modus installieren.

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

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

Sie können die automatischen Datenbanken-Updates nach dem Abschluss der Ersteinrichtung der Anwendung aktivieren, indem Sie einen Zeitplan für die Update-Aufgabe einrichten.

Schritt 20. App aktivieren

Dieser Schritt wird angezeigt, wenn Sie Kaspersky Endpoint Security im Standard-Modus oder im EDR-Agent-Modus installieren.

Wenn Sie das Programm sofort nach der Installation aktivieren möchten, geben Sie einen Aktivierungscode ein oder geben Sie den vollständigen Pfad zu einer Schlüsseldatei an.

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

Sie können die Anwendung stets später aktivieren, nachdem Sie die Ersteinrichtung der Anwendung abgeschlossen haben.

So führen Sie die Erstkonfiguration im automatischen Modus durch

1. Erstellen Sie eine Konfigurationsdatei, die die Einstellungen für die Erstkonfiguration enthält. Sie können die Einstellungen aus der Konfigurationsdatei autoinstall.ini kopieren, die für die Remote-Installation des Programms mithilfe von Kaspersky Security Center verwendet wird, und bei Bedarf Änderungen vornehmen.

2. Geben Sie die folgenden erforderlichen Einstellungen in der Konfigurationsdatei an:

   - Akzeptieren des Endbenutzer-Lizenzvertrags (EULA) und der Datenschutzrichtlinie:

     `EULA_AGREED=Yes`

     `PRIVACY_POLICY_AGREED=Yes`

     Sie können die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie in der Datei license.<language ID> lesen, die im Lieferumfang des Programms enthalten ist:

     > Wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie nicht akzeptieren, wird der Installationsvorgang abgebrochen.

   - Die Kaspersky Security Network-App wird standardmäßig im Standard-Modus verwendet.

     Um das Programm im EDR-Agent-Modus zu verwenden, geben Sie die folgende Einstellung an:

     `ENDPOINT_AGENT_MODE=Yes`

     Um das Programm im Light Agent-Modus zu verwenden, geben Sie die folgende Einstellung an:

     `KSVLA_MODE=Yes`

   - Verwendung von Kaspersky Security Network Akzeptieren oder Ablehnen der Nutzungsbedingungen für Kaspersky Security Network:

     `USE_KSN=Yes|No`

     Die Datei "ksn_licence.<Sprach-ID>", die den Text der Erklärung zu Kaspersky Security Network enthält, befindet sich im Verzeichnis opt/kaspersky/kesl/doc/. Wenn Sie die Bedingungen der Erklärung zu Kaspersky Security Network akzeptieren, wird der erweiterte KSN-Modus aktiviert. Sie können den Modus von Kaspersky Security Network jederzeit aktivieren, deaktivieren oder ändern.

     > Wenn Kaspersky Security Network aktiviert ist, wird automatisch der Cloud-Modus aktiviert, in dem Kaspersky Endpoint Security die schlanke Version der Malware-Datenbanken verwendet.

   - Automatisches Entfernen von Benutzern aus den privilegierten Gruppen kesladmin und keslaudit vor der Installation des Programms:

     `GROUP_CLEAN=Yes|No`

3. Wählen Sie den von Kaspersky Endpoint Security verwendeten Mechanismus zum Abfangen von Systemereignissen aus. Wenn Sie das aktualisierbare Kernel-Modul zum Abfangen von Systemereignissen verwenden möchten, legen Sie den folgenden Wert fest:

   `INTERCEPTOR_MODE=UseUpdatableKernelModule`

   Standardmäßig wird die fanotify-Technologie zum Abfangen von Systemereignissen verwendet.

4. Wenn Sie das Programm im Standard-Modus oder im EDR-Agent-Modus installieren, geben Sie die folgenden Einstellungen an:

   - Proxyserver-Einstellungen. Wenn Sie für Ihre Internetverbindung einen Proxyserver verwenden, geben Sie die Adresse Ihres Proxyservers in einem der folgenden Formate ein:

     - `PROXY_SERVER=[<connection protocol>://]<address of proxy server>:<port>`, wenn für die Verbindung mit dem Proxyserver keine Authentifizierung erforderlich ist;

     - `PROXY_SERVER=[<connection protocol>://][<user name>:<password>@]<address of proxy server>:<port>`, wenn für die Verbindung mit dem Proxyserver eine Authentifizierung erforderlich ist. Geben Sie eine IPv6-Adresse in eckigen Klammern ein.

     > Das Herstellen einer Verbindung mit dem Proxyserver über das HTTPS-Protokoll wird nicht unterstützt.

   - Installieren und Verwenden der grafischen Oberfläche des Programms:

     `USE_GUI=Yes|No`

5. Wenn Sie das Programm im Light Agent-Modus installieren, geben Sie die folgenden Einstellungen an:

   - Rolle der geschützten virtuellen Maschine:

     - `SERVER_MODE=Yes`, wenn die geschützte virtuelle Maschine als Server verwendet wird.

     - `SERVER_MODE=No`, wenn die geschützte virtuelle Maschine als Workstation verwendet wird.

   - Aktivieren des Modus zum Schutz der VDI-Infrastruktur, um die Leistung der App auf temporären virtuellen Maschinen zu optimieren. Wenn Sie das Programm auf einer Vorlage für virtuelle Maschinen installieren, aus der temporäre virtuelle Maschinen erstellt werden, legen Sie den folgenden Wert fest:

     `VDI_MODE=Yes`

6. Starten Sie den Assistenten für die Ersteinrichtung:

   ```
   /opt/kaspersky/kesl/bin/kesl-setup.pl --autoinstall=<initial configuration file>
   ```

   Dabei ist `<initial configuration file>` der Pfad zur Konfigurationsdatei mit den Einstellungen für die Ersteinrichtung.

Wenn der Assistent zur Erstkonfiguration abgeschlossen ist und die Befehlszeile freigibt, ist der Prozess der Erstkonfiguration der Anwendung beendet.

Rückgabecode überprüfen

```
echo $?
```

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

Wenn beim ersten Update der Datenbanken und Module innerhalb von 24 Stunden nach der Installation des Programms kritische Updates empfangen werden, wird das Programm automatisch neu gestartet.

4 Überprüfung der Programmgesundheit

Dadurch wurde das Programm Kaspersky Endpoint Security installiert und aktiviert, und die Programmdatenbanken wurden aktualisiert. Nach der Installation wird das Programm automatisch gestartet. Standardmäßig sind die folgenden Komponenten aktiviert:

- 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.

Überprüfen des Schutzstatus des Geräts für den Standard-Modus

Führen Sie den folgenden Befehl aus, um den Schutzstatus des Geräts zu überprüfen:

```
kesl-control --app-info [--json]
```

Dabei bedeutet `--json` die Ausgabe von Daten im JSON-Format. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen in die Konsole ausgegeben.

Stellen Sie sicher, dass:

- Das Programm ist aktiviert (Zeile **Informationen zur Lizenz der Anwendung**).
- Die Programmdatenbanken sind auf dem neuesten Stand (Zeilen **Programm-Datenbanken geladen** und **Veröffentlichungsdatum der verwendeten Programm-Datenbanken**).
- Der Schutz vor bedrohlichen Dateien ist aktiviert (Zeile **Schutz vor bedrohlichen Dateien**).
- In der Zeile **Programmstatus** wird `OK` angezeigt.

  Wenn in der Zeile **Programmstatus** Informationen über unzureichende Rechte für Systemverzeichnisse angezeigt werden, überprüfen Sie lokal auf diesem Gerät die Berechtigungen für die folgenden Verzeichnisse: /var/opt/kaspersky, /var/log/kaspersky und /opt/kaspersky. Stellen Sie sicher, dass der Besitzer root ist und nur der Besitzer Schreibzugriff auf diese Verzeichnisse hat.

Überprüfen des Schutzstatus des Geräts für den EDR Agent-Modus

Führen Sie den folgenden Befehl aus, um den Schutzstatus des Geräts zu überprüfen:

```
kesl-control --app-info [--json]
```

Dabei bedeutet `--json` die Ausgabe von Daten im JSON-Format. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen in die Konsole ausgegeben.

Stellen Sie sicher, dass:

- Das Programm ist aktiviert (Zeile **Lizenzinformation zu EDR Expert (on-premise)**)
- Die Programmdatenbanken sind auf dem neuesten Stand (Zeilen **Programm-Datenbanken geladen** und **Veröffentlichungsdatum der verwendeten Programm-Datenbanken**).
- Das Programm wird im EDR Agent-Modus verwendet (Zeile **Modus als Endpoint Detection and Response Agent**).
- Für die Integrationen, die Sie in der Richtlinie konfiguriert haben, wird der Status „Verfügbar und wird ausgeführt“ angezeigt.
- In der Zeile **Programmstatus** wird `OK` angezeigt.

  Wenn in der Zeile **Programmstatus** Informationen über unzureichende Rechte für Systemverzeichnisse angezeigt werden, überprüfen Sie lokal auf diesem Gerät die Berechtigungen für die folgenden Verzeichnisse: /var/opt/kaspersky, /var/log/kaspersky und /opt/kaspersky. Stellen Sie sicher, dass der Besitzer root ist und nur der Besitzer Schreibzugriff auf diese Verzeichnisse hat.

Überprüfen des Schutzstatus des Geräts für den Light Agent-Modus

1. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control --ksvla-info
   ```

   Stellen Sie sicher, dass das Programm im Light Agent-Modus verwendet wird (Zeile **Light Agent-Modus zum Schutz virtueller Umgebungen**).

2. Wenn Sie in der Richtlinie einen Integrationsserver ausgewählt haben, um für die Verbindung verfügbare SVMs zu erkennen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --viis-info
   ```

   Stellen Sie sicher, dass Light Agent mit dem Integrationsserver verbunden ist (Zeile **Status der Verbindung zum Integrationsserver**).

3. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control --svm-info
   ```

   Stellen Sie sicher, dass Light Agent mit der SVM verbunden ist: Es werden Informationen über die SVM angezeigt, zu der eine Verbindung hergestellt wurde.

4. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control --app-info [--json]
   ```

   Dabei bedeutet `--json` die Ausgabe von Daten im JSON-Format. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen in die Konsole ausgegeben.

Stellen Sie sicher, dass:

- Der Light Agent erhält Informationen über die Lizenz, mit der Kaspersky Security for Virtualization Light Agent aktiviert wurde (Zeile **Informationen zur Lizenz der Anwendung**).
- Die Programmdatenbanken sind auf dem neuesten Stand (Zeilen **Programm-Datenbanken geladen** und **Veröffentlichungsdatum der verwendeten Programm-Datenbanken**).
- In der Zeile **Programmstatus** wird `OK` angezeigt.

  Wenn in der Zeile **Programmstatus** Informationen über unzureichende Rechte für Systemverzeichnisse angezeigt werden, überprüfen Sie lokal auf diesem Gerät die Berechtigungen für die folgenden Verzeichnisse: /var/opt/kaspersky, /var/log/kaspersky und /opt/kaspersky. Stellen Sie sicher, dass der Besitzer root ist und nur der Besitzer Schreibzugriff auf diese Verzeichnisse hat.

Nützliche Artikel

Vorgehensweise, wenn Aufgaben nicht ausgeführt oder Richtlinien nicht angewendet werden

Vorgehensweise, wenn das Gerät den folgenden Status aufweist: „Ungültige Richtlinieneinstellungen. Richtlinie wurde nicht angewendet."

Fehler: „Die App wird von der aktuellen Version von Kaspersky Security Center Web Console nicht unterstützt oder das Web-Plug-in der App ist nicht installiert"

Beheben eines Problems bei der Installation der grafischen Benutzeroberfläche

Beschreibung der Installationsfehlercodes

Fehler nach der Installation von Kaspersky Endpoint Security

Nachdem Sie Kaspersky Endpoint Security installiert haben, können Sie zum Bereitstellungsszenario zurückkehren und mit dem Schritt Zusätzliche Konfigurationsschritte nach der Installation unter bestimmten Betriebssystemen fortfahren.

Zusätzliche Konfigurationsschritte nach der Installation in bestimmten Betriebssystemen

Nach Vorbereitung der Umgebung für die Installation von Kaspersky Endpoint Security und nach der Installation des Programms ist für einige Betriebssysteme eine zusätzliche Konfiguration erforderlich.

Manuelle Konfiguration von SELinux für die Arbeit mit der Anwendung

Wenn Ihr Betriebssystem das Zugriffskontrollsystem SELinux im Modus `Enforcing` verwendet, wird es während der Installation standardmäßig automatisch für die Verwendung mit dem Programm konfiguriert.

Wenn das Programm SELinux nicht automatisch konfigurieren kann (z. B. wenn das Hilfsprogramm semanage fehlt), zeigt der Assistent eine Fehlermeldung an und fordert den Benutzer auf, SELinux manuell zu konfigurieren. Konfigurieren Sie in diesem Fall oder wenn Sie die automatische Konfiguration abgelehnt haben nach Abschluss der Erstkonfiguration des Programms das SELinux-System manuell für die Verwendung mit dem Programm Kaspersky Endpoint Security.

Diese Konfiguration erfordert Root-Rechte.

So konfigurieren Sie das SELinux-System für die gemeinsame Ausführung mit der Anwendung manuell:

1. Versetzen Sie das SELinux-System in den Erlaubnismodus:

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

     ```
     setenforce Permissive
     ```

   - Wenn SELinux deaktiviert ist, legen Sie `SELINUX=permissive` in der Konfigurationsdatei /etc/selinux/config fest 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 anstelle der standardmäßigen Richtlinie 'targeted' eine benutzerdefinierte SELinux-Richtlinie verwenden, weisen Sie jeder ursprünglichen ausführbaren Datei von Kaspersky Endpoint Security gemäß Ihrer SELinux-Richtlinie ein Label zu.

   ```
   semanage fcontext -a -t bin_t <executable file>
   restorecon -v <executable file>
   ```

   Dabei ist `<executable file>`:

   - /var/opt/kaspersky/kesl/<Build-Nummer_*>/opt/kaspersky/kesl/libexec/kesl
   - /var/opt/kaspersky/kesl/<Build-Nummer_*>/opt/kaspersky/kesl/bin/kesl-control
   - /var/opt/kaspersky/kesl/<Build-Nummer_*>/opt/kaspersky/kesl/libexec/kesl-gui
   - /var/opt/kaspersky/kesl/<Build-Nummer_*>/opt/kaspersky/kesl/shared/kesl
   - /var/opt/kaspersky/kesl/<Build-Nummer_*>/opt/kaspersky/kesl/bin/response

4. Führen Sie den folgenden Aufgaben aus:

```
Aufgabe zum Schutz vor bedrohlichen Dateien starten
```

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

```
Aufgabe zur Untersuchung wichtiger Bereiche starten
```

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

> Es wird empfohlen, alle Aufgaben von Kaspersky Endpoint Security auszuführen, die Sie zukünftig ausführen möchten.

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

6. Stellen Sie sicher, dass die Datei audit.log keine Fehler enthält.

```
Datei audit.log anzeigen
```

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

7. Wenn die Datei audit.log Fehler enthält, erstellen Sie auf Basis der blockierenden Einträge ein neues Regelmodul und laden Sie es herunter, um die Fehler zu beheben. Starten Sie anschließend alle Aufgaben, die Sie zukünftig ausführen möchten, erneut.

```
Erstellen und laden Sie ein neues Regelmodul basierend auf blockierenden Einträgen:
```

```
grep kesl /var/log/audit/audit.log | audit2allow -M kesl
semodule -i kesl.pp
```

> 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 Modus „enforcing“ um.

```
setenforce Enforcing
```

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

Weitere Informationen finden Sie in der Dokumentation des jeweiligen Betriebssystems.

SELinux für Reaktionsaktionen konfigurieren

Wenn Sie SELinux auf Ihrem Betriebssystem im Modus `Enforcing` verwenden möchten, müssen Sie zur Ausführung von Reaktionsaktionen bei der Integration mit Detection and Response-Lösungen zusätzlich die SELinux-Einstellungen verwalten.

Diese SELinux-Konfiguration erfordert Root-Rechte.

So konfigurieren Sie SELinux für Reaktionsaktionen:

1. Versetzen Sie das SELinux-System in den Erlaubnismodus:
   - Wenn SELinux aktiviert ist, führen Sie den folgenden Befehl aus:

     SELinux in den Modus „permissive“ umschalten

     ```
     setenforce Permissive
     ```

   - Wenn SELinux deaktiviert ist, legen Sie `SELINUX=permissive` in der Konfigurationsdatei /etc/selinux/config fest 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 alle Aufgaben aus, um die Reaktionsaktionen durchzuführen, die Sie im Rahmen der Integration mit Detection and Response-Lösungen verwenden möchten.
4. Um mithilfe der Aufgaben „Speicherabbild abrufen“ und „Prozessspeicherabbild abrufen“ forensische Daten zu erfassen, erlauben Sie der Anwendung Kaspersky Endpoint Security in SELinux den Zugriff auf die in den Aufgaben angegebenen SMB-Server.
5. Stellen Sie sicher, dass die Datei audit.log keine Fehler enthält.

   Datei audit.log anzeigen

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

6. Wenn die Datei audit.log Fehler enthält, erstellen und laden Sie ein neues Regelmodul auf Basis der blockierenden Einträge, um die Fehler zu beheben. Führen Sie anschließend die Aufgaben für Reaktionsaktionen erneut aus.

   Erstellen und laden Sie ein neues Regelmodul basierend auf blockierenden Einträgen:

   ```
   grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   semodule -i kesl.pp
   ```

7. Schalten Sie SELinux in den Modus „enforcing“ um.

   ```
   setenforce Enforcing
   ```

Konfiguration des Programmstarts im Betriebssystem OSnova

Führen Sie nach der Installation des Programms die folgenden Schritte aus, um das Programm zu starten:

1. Öffnen Sie die Datei `/etc/NESS/systemd/kesl.service.config` und legen Sie `NESSCTX_MODIFY="t+ADDEQUSOCK,OMIT,OMIT_PID,SSUID_SAVE_CTX_PERMANENT"` fest.

2. Öffnen Sie die Datei `/etc/sysctl.d/30-disable-ptrace.conf` und legen Sie `kernel.yama.ptrace_scope=0` fest. Andere Werte des Parameters `kernel.yama.ptrace_scope` können sich auf den Betrieb von Kaspersky Endpoint Security auswirken. Weitere Informationen finden Sie im Abschnitt Bekannte Probleme und Einschränkungen.

3. Wenn Sie eine Untersuchung des Prozessspeichers und des Kernel-Speichers ausführen möchten, müssen Sie den Speicherschutzmechanismus mprotect (oder PaX) im Kernel deaktivieren. Fügen Sie dazu die Option `mprotect=off` zur Befehlszeile des Kernels hinzu. Weitere Informationen dazu finden Sie in der Dokumentaion zu OSnova.

4. Starten Sie das Betriebssystem neu.

Konfiguration des Starts des Programms auf ALT SP im Modus der geschlossenen Softwareumgebung

Führen Sie nach der Installation des Programms die folgenden Schritte aus, um das Programm zu starten:

1. Legen Sie die Vererbung der Gruppe kesl und die Verzeichnisberechtigungen für die aktualisierbaren Komponenten von Kaspersky Endpoint Security fest:

```
cd /var/opt/kaspersky/kesl/<build number_*>/var/opt/kaspersky/kesl/private
chown -R root:kesl updates/
find updates -type d -exec chmod g+s {} \;
cd /opt/kaspersky/kesl/lib64
chown -R root:kesl updatable_modules/
find updatable_modules -type d -exec chmod g+s {} \;
cd /var/opt/kaspersky/kesl/common/
chown -R root:kesl temp/
find temp -type d -exec chmod g+s {} \;
```

2. Legen Sie die Vererbung der Gruppe kesl und die Verzeichnisberechtigungen für die aktualisierbaren Komponenten des Administrationsagenten fest:

```
cd /var/opt/kaspersky/
chown -R root:kesl klnagent/
find klnagent/ -type d -exec chmod g+s {} \;
cd /opt/kaspersky/
chown -R root:kesl klnagent64/
find klnagent64/ -type d -exec chmod g+s {} \;
```

3. Aktivieren Sie den Modus der geschlossenen Softwareumgebung, indem Sie die Signierung des Systems initiieren:

```
integrity-applier -i -A
```

4. Stellen Sie sicher, dass das IMA-Subsystem aktiviert ist:

```
cat /proc/cmdline
```

Die Ausgabe des Befehls sollte die Zeilen `lsm=integrity ima_hash=sha512 ima_appraise=enforce` enthalten.

5. Führen Sie die Aufgabe zum Datenbanken-Update aus:

```
kesl-control --start 6 -W
```

Wenn die Ausgabe der Aufgabe zum Datenbanken-Update ein Ereignis *EventType=BasesApplied* enthält, bedeutet dies, dass das Datenbanken-Update korrekt ausgeführt wurde.

6. Starten Sie das Programm neu:

```
systemctl restart kesl
```

Migrationsszenario zu Kaspersky Security Center für Linux mithilfe des Schnellinstallationsskripts

Dieses Szenario enthält Beispiele für die folgenden Anwendungsfälle der Migration der Lösung mit Daten auf ein neues Gerät für den Administrationsserver:

- Migration von Kaspersky Security Center Windows (MS SQL und PostgreSQL) zu Kaspersky Security Center Linux (PostgreSQL).
- Migration von Kaspersky Security Center Linux (PostgreSQL) zum Ersetzen der Hardware.

Der neue Administrationsserver wird mithilfe des Schnellinstallationsskripts bereitgestellt.

Weitere Möglichkeiten zur Datenübertragung werden im Abschnitt über die Migration zu Kaspersky Security Center Linux beschrieben.

1 Voraussetzungen für das Erstellen einer Backup-Kopie

Dieser Schritt enthält eine Anleitung zur Vorbereitung eines zuvor konfigurierten Administrationsservers für die anschließende Migration auf einen neuen Administrationsserver von Kaspersky Security Center Linux. Der Vorbereitungsprozess umfasst die folgenden Schritte:

1. Überprüfen der Version des Administrationsservers, um eine mit Kaspersky Security Center Linux kompatible Backup-Kopie zu erstellen.

   Alle aktuellen Versionen von **Kaspersky Security Center Linux** unterstützen die Datenmigration mit einem Upgrade des Programms auf eine neuere Version. Backup-Kopien können nur innerhalb desselben DBMS-Typs erstellt und wiederhergestellt werden.

   Für **Kaspersky Security Center Windows** müssen Sie die Version des Administrationsservers unter **Eigenschaften** → **Allgemein** → **Version** überprüfen. Wenn die Version älter als 15.1.0.22239 ist, führen Sie für Kaspersky Security Center Windows ein Upgrade auf die neueste Version durch.

Upgrade von Kaspersky Security Center für Windows auf die neueste Version.

1. Laden Sie auf der Kaspersky-Website das Programmpaket herunter, das der Lokalisierungssprache des installierten Administrationsservers entspricht: `Version 15.1.0.22239 | Windows | Full distributive`.

   Die ausführbare Datei wird im Ordner **Downloads** unter folgendem Namen gespeichert: `ksc_15.1_<build number>_full_<language>.exe`.

2. Kopieren Sie das Programmpaket auf den Administrationsserver.

3. Führen Sie die ausführbare Datei `ksc_15.1_<build number>_full_<language>.exe` als Administrator aus.

4. Klicken Sie im angezeigten Fenster auf den Link **Kaspersky Security Center installieren**.

   Der Setup-Assistent für den Administrationsserver wird gestartet.

5. Lesen Sie den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie. Wenn Sie mit allen Bestimmungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind, aktivieren Sie im Abschnitt **Ich bestätige, dass ich die folgenden Dokumente vollständig gelesen habe, und sie verstehe und akzeptiere** die folgenden Kontrollkästchen:

   - **Bestimmungen und Bedingungen dieser EULA**.
   - **Datenschutzrichtlinie, in der die Datenverarbeitung beschrieben wird**.

6. Wählen Sie **Upgrade des Administrationsservers und der webbasierten Konsole (empfohlen)** aus und fahren Sie mit dem nächsten Schritt fort.

7. Erstellen Sie eine neue Backup-Kopie, wählen Sie die Option **Ich möchte eine Backup-Kopie der Daten anlegen** aus und befolgen Sie die Schritte des Backup-Assistenten.

8. Klicken Sie auf die Schaltfläche **Upgrade**.

9. Bestätigen Sie während des Upgrades im Installationsassistenten der Web Console alle Schritte zum Upgrade der Version.

   Die Installation des Upgrades für den Administrationsserver dauert einige Zeit. Nach Abschluss des Installationsassistenten nimmt die Verwaltungskonsole möglicherweise keine Verbindungen an, bis die Initialisierung der Datenbank abgeschlossen ist.

10. Warten Sie, bis das Upgrade abgeschlossen ist.

2. Überprüfung der Einhaltung der Anforderungen an das Zertifikat des Administrationsservers.

   Bevor Sie eine Backup-Kopie erstellen, müssen Sie sicherstellen, dass das Zertifikat Subject Alternative Name (SAN) enthält. Ist dies nicht der Fall, ersetzen Sie unbedingt das Zertifikat, da Sie sich andernfalls nach der Wiederherstellung aus einem Backup nicht mehr bei der Web Console anmelden können.

So überprüfen Sie, ob das Zertifikat den alternativen Antragstellernamen enthält:

- Für Geräte mit Windows:

  a. Wählen Sie in der Verwaltungskonsole den Administrationsserver aus, den Sie überprüfen möchten.

  b. Wählen Sie im Kontextmenü **Eigenschaften → Allgemein → Zertifikat des Administrationsservers anzeigen** aus.

  c. Daraufhin wird ein Fenster geöffnet. Überprüfen Sie in diesem Fenster den Wert des Elements **Alternativer Antragstellername**.

- Führen Sie für ein Linux-Gerät den folgenden Befehl aus:

```
sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
```

Stellen Sie sicher, dass der alternative Antragstellername den Domänennamen (DNS) des Geräts mit dem Administrationsserver enthält.

Wenn der Wert nur eine externe IP-Adresse ohne Domänennamen (DNS) enthält oder der Wert vollständig fehlt, ersetzen Sie das Zertifikat manuell durch ein Zertifikat, das den Anforderungen von Kaspersky Security Center Linux entspricht. Ersetzen Sie das allgemeine Zertifikat des Administrationsservers mithilfe des Dienstprogramms klsetsrvcert.

Ersetzen des allgemeinen Zertifikats des Administrationsservers mithilfe des Dienstprogramms klsetsrvcert

1. Erstellen Sie auf den Geräten ein neues Zertifikat mit einem späteren Startdatum, indem Sie den folgenden Befehl ausführen:

   - Für Kaspersky Security Center Windows:

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
     <oldksc.example.internal>" -o "RsaKeyLen:2048"
     ```

   - Für Kaspersky Security Center Linux:

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
     ```

   wobei `"<oldksc.example.internal>"` der FQDN für die Verbindung zum Administrationsserver ist.

   > Verwenden Sie für diesen Wert keine IP-Adresse.

2. Legen Sie das Startdatum für das neue Zertifikat auf allen Geräten fest, indem Sie den folgenden Befehl ausführen:

   - Für Kaspersky Security Center Windows:

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
     ```

- Für Kaspersky Security Center Linux:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
```

wobei `"DD-MM-YYYY hh:mm"` ein Datum ist, das mindestens 30 Tage nach dem aktuellen Datum liegt. Standardmäßig beträgt der Verteilungszeitraum für ein neues Zertifikat (`CR`) 90 Tage.

> Wenn der festgelegte Zeitpunkt erreicht ist, müssen Sie die Web Console neu installieren, um den Zugriff darauf wiederherzustellen und ihr Zertifikat zu aktualisieren.

3. Führen Sie bei Bedarf nach der Migration zum neuen Administrationsserver das Dienstprogramm klmover aus, um die Verbindung der Geräte zum Administrationsserver wiederherzustellen. Sie müssen dieses Dienstprogramm möglicherweise starten, wenn ein Gerät während des gesamten Zeitraums der Zertifikatsverteilung ausgeschaltet war oder noch nie mit dem Administrationsserver verbunden war.

2 Erstellen einer Backup-Kopie der vorherigen Installation des Administrationsservers

Erstellen einer Backup-Kopie von Kaspersky Security Center Windows

1. Führen Sie über **Startmenü** → **Kaspersky Security Center** → **Kaspersky Backup-Dienstprogramm** das Dienstprogramm `klbackup.exe` aus, das sich im Installationsordner von Kaspersky Security Center Linux befindet.

   Der Setup-Assistent wird gestartet. Verwenden Sie unter Microsoft Windows im Server Core-Modus die Konsolenversion des Dienstprogramms klbackup.

2. Wählen Sie im ersten Schritt **Backup der Daten des Administrationsservers durchführen** aus.

3. Im Schritt **Backup-Einstellungen**:

   a. Klicken Sie auf die Schaltfläche **Durchsuchen** und erstellen Sie einen neuen Ordner, um die Backup-Kopie getrennt vom Standardverzeichnis zu speichern, z. B. `C:\kscbackups`.

   b. Wenn Sie Microsoft SQL Server verwenden, wählen Sie die Option **Datenbank migrieren** → **Zu Postgres migrieren** aus, um ihn mit dem Schnellinstallationsskript zu verwenden. Wenn Sie Kaspersky Security Center Linux mit der Standardmethode bereitstellen, können Sie Daten auch in eine MySQL-/MariaDB-Datenbank migrieren.

   c. Legen Sie ein Kennwort für die Backup-Kopie fest, um sie vor unbefugtem Zugriff auf die Daten zu schützen.

4. Warten Sie, bis die Backup-Kopie erstellt wurde, und beenden Sie das Dienstprogramm.

Im angegebenen Verzeichnis wird ein neues Unterverzeichnis mit dem Zeitstempel des Backups erstellt.

Erstellen einer Backup-Kopie von Kaspersky Security Center Linux

1. Führen Sie auf dem Gerät mit dem Administrationsserver den folgenden Befehl in der Befehlszeile aus:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klbackup -path /root/kscbackups -use_ts
   ```

2. Warten Sie, bis der Backup-Vorgang abgeschlossen ist.

   Ein neues Unterverzeichnis mit dem Zeitstempel des Backups wird in dem Verzeichnis erstellt, das in der Option `-path` angegeben ist.

Nachdem Sie eine Backup-Kopie Ihres bisherigen Administrationsservers erstellt haben, nehmen Sie das Gerät mit dem Administrationsserver außer Betrieb.

Außerbetriebnahme des Geräts mit dem Administrationsserver

1. Kopieren Sie die erhaltene Backup-Kopie für die Datenmigration auf das Gerät des Administrators.
2. Fahren Sie das Betriebssystem des Administrationsservers herunter.
3. Trennen Sie den Netzwerkadapter vom Unternehmensnetzwerk.
4. Geben Sie die IP-Adresse des Geräts frei, wenn Sie sie für die Neuinstallation von Kaspersky Security Center Linux wiederverwenden möchten.
5. Stellen Sie sicher, dass das Gerät vollständig ausgeschaltet ist.

Der im Netzwerk verbleibende alte Administrationsserver kann Fehler bei der Geräteverwaltung verursachen, den Anmeldevorgang an der Web Console des neuen Administrationsservers stören und außerdem dazu führen, dass die Installationsaufgabe für den Administrationsagenten mit einer Verbindung zum alten Server gestartet wird.

3 Erstbereitstellung von Kaspersky Security Center Linux mithilfe des Schnellinstallationsskripts

Diese Anleitung beschreibt die Erstbereitstellung einer Instanz von Kaspersky Security Center Linux mithilfe des Schnellinstallationsskripts.

Besonderheiten:

- Alle Komponenten von Kaspersky Security Center werden auf demselben Gerät wie der Administrationsserver installiert.
- Das Betriebssystem des Administrationsservers muss eines der folgenden Betriebssysteme sein:
  - Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.8.5) mit PostgreSQL 15
  - Ubuntu Server 26.04 LTS mit PostgreSQL 18

- CentOS Stream 10 mit PostgreSQL 18
- RED OS 8.0 mit PostgreSQL 16

- Das Schnellinstallationsskript automatisiert nur die Konfiguration und Installation des Programms Kaspersky Security Center. Der Administrator muss Maßnahmen ergreifen, um den Namen des Geräts mit dem Administrationsserver im Betriebssystem, die Netzwerkadapter und Sicherheits-Firewalls auf Betriebssystemebene sowie die Hardware zu konfigurieren.

Die Erstbereitstellung einer Instanz von Kaspersky Security Center Linux mithilfe des Schnellinstallationsskripts umfasst die folgenden Schritte:

1. Vorbereitung auf die Bereitstellung

Bevor Sie mit den Installationsschritten fortfahren, müssen Sie Folgendes vorbereiten:

- Ein Installationsdatenträgerabbild des Betriebssystems und ein Repository mit Programmpaketen.
- Eine Authentifikator-App für die Zwei-Faktor-Authentifizierung (2FA) bei der Anmeldung an der Web Console.
- Ein neuer FQDN (z. B. *ksclinux.example.com*). Wenn Sie über ausreichende Erfahrung mit der Konfiguration von Lösungen verfügen, können Sie Ihr eigenes Skript verwenden, um dem neuen Server während der Installation den vorherigen FQDN zuzuweisen. Überspringen Sie in diesem Fall in Schritt 5 „Programm nach der Wiederherstellung aus einer Backup-Kopie konfigurieren“ den Schritt 4. Verbindung der verwalteten Geräte mit dem FQDN des vorherigen Administrationsservers wiederherstellen
- Ein Administratorgerät mit einem Browser zum Herunterladen von Distributionen und zum Verwalten der Web Console über das Internet.
- Stellen Sie die Verfügbarkeit von DNS und eines Zeitservers (NTP) für Programmkomponenten sicher.
- Geben Sie je nach Szenario die vorherige IP-Adresse frei, wenn sie zum Verbinden verwalteter Geräte verwendet wurde.
- Konfigurieren Sie die Netzwerkgeräte und den Proxyserver gemäß den Anforderungen:
  - Ports für die Kommunikation zwischen Programmkomponenten.
  - Zugriff auf Kaspersky-Server.
  - Empfehlungen aus dem Hardening Guide.

2. Dimensionierung und Konfiguration des Betriebssystems

1. Konfigurieren Sie die Hardware entsprechend der Anzahl der Geräte, die der Administrationsserver verwalten soll.

   Bei jeder Berechnung der Dimensionierung werden die verfügbaren Ressourcen für Kaspersky-Programme berücksichtigt. Die Berechnung berücksichtigt, dass Administrationsserver, Administrationsagent, DBMS, Server der Web Console und Kaspersky Endpoint Security für Linux auf demselben Gerät ausgeführt werden. Bei der Berechnung wird jedoch die Speicherung von Backup-Kopien des Administrationsservers nicht berücksichtigt.

   > Verwenden Sie eine externe Dateifreigabe als Einhängepunkt, um Backup-Kopien auf einem separaten Gerät zu speichern, oder erhöhen Sie die Anforderung an den freien Festplattenspeicher unter Berücksichtigung der Speicherung von Backups.

Wir empfehlen, zusätzlich 4–6 GB RAM und 20 GB freien Festplattenspeicher für das Betriebssystem einzuplanen.

Dimensionierung des Geräts abhängig von der Anzahl der verwalteten Geräte:

- **S** (bis zu 1000 Geräte): 8 CPU-Kerne, 16 GB RAM, 70 GB freier Festplattenspeicher für das Verzeichnis `/var`, 300 IOPS oder mehr.
- **M** (bis zu 10.000 Geräte): 12 CPU-Kerne, 24 GB RAM, 340 GB freier Festplattenspeicher für das Verzeichnis `/var`, 300 IOPS oder mehr.
- **L** (bis zu 30.000 Geräte): 20 CPU-Kerne, 40 GB RAM, 490 GB freier Festplattenspeicher für das Verzeichnis `/var`, 300 IOPS oder mehr.
- **XL** (bis zu 50.000 Geräte): 28 CPU-Kerne, 54 GB RAM, 640 GB freier Festplattenspeicher für das Verzeichnis `/var`, 300 IOPS oder mehr.

2. Bereiten Sie die Hardware für den Kaspersky Security Center-Server gemäß den ausgewählten Spezifikationen vor.

3. Installieren Sie das Betriebssystem auf dem Kaspersky Security Center-Server.

   Aktivieren Sie während der Installation die Option **SSH-Tools für Remote-Verbindungen**, wenn Sie das Gerät des Administrationsservers remote über die Befehlszeile verwalten möchten.

   > Astra Linux muss mit deaktivierter Option **Obligatorische Zugriffskontrolle** installiert werden. Damit Kaspersky Endpoint Security für Linux ordnungsgemäß funktioniert, deaktivieren Sie außerdem die Option **ptrace-Ablaufverfolgung blockieren**.

4. Überprüfen Sie den freien Speicherplatz für das Verzeichnis `/var`, wenn es separat eingehängt ist, oder für das Stammverzeichnis `/`.

   Beispiele für eine M-Konfiguration:

   Astra Linux

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                 Size  Used Avail Use% Mounted on
   /dev/mapper/astra48242-01  406G  8,0G 377G    3% /
   <...>
   ```

   Ubuntu

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                         Size  Used Avail Use% Mounted on
   /dev/mapper/ubuntu--vg-ubuntu--lv  406G   11G  374G   3% /
   <...>
   ```

5. Konfigurieren Sie auf dem neuen Server die IP-Adresse des vorherigen Administrationsservers, wenn für die Verbindung mit verwalteten Geräten eine IP-Adresse verwendet wurde.

Video: Konfiguration des Betriebssystems



3. Herunterladen der Distributionsdateien

1. Laden Sie die Programmpakete für das gewünschte Gebietsschema von der Kaspersky-Website herunter und speichern Sie sie in einem separaten Verzeichnis (z. B. *kscdistr*).

   Für Ubuntu und Astra Linux

   - Programmpaket des Administrationsservers im deb-Format:
     `Version 16.3.0.1207 | Debian x64 | Administration server`
   - Programmpaket der Web Console im deb-Format:
     `Version 16.3.0.1207 | Debian x64 | Web console`
   - Skript für die Schnellinstallation:
     `Version 16.3.0.1207 | Linux | KSC installation script`

   Für CentOS und RED OS

   - Programmpaket des Administrationsservers im rpm-Format:
     `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Administration server`
   - Programmpaket der Web Console im rpm-Format:
     `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Web console`
   - Skript für die Schnellinstallation:
     `Version 16.3.0.1207 | Linux | KSC installation script`

2. Damit Kaspersky-Programme im Modus der geschlossenen Softwareumgebung von Astra Linux ausgeführt werden können, laden Sie die öffentliche Schlüsseldatei kaspersky_astra_pub_key.gpg herunter.

3. Kopieren Sie die heruntergeladenen Dateien mithilfe von Wechseldatenträgern oder über das Netzwerk auf das neue Gerät des Kaspersky Security Center Administrationsservers.

   Im Folgenden werden die Aktionen für das Kopieren über das Netzwerk mithilfe der Befehlszeile beschrieben.

Ob Sie das Dienstprogramm scp zum Kopieren der Dateien verwenden können, hängt davon ab, ob im Betriebssystem des Geräts des Administrationsservers ein SSH-Dienst ausgeführt wird, sowie von der Sicherheitsrichtlinie Ihrer Organisation.

a. Wechseln Sie in der Befehlszeile mit dem Befehl cd in das Verzeichnis, das eine Ebene über dem Verzeichnis *kscdistr* liegt, zum Beispiel:

Für Linux

```
cd /home/administrator/Desktop
```

Für Windows

```
cd C:\Users\Administrator\Downloads
```

b. Kopieren Sie die Distributionsdateien mithilfe des Dienstprogramms scp über das Netzwerk:

```
scp -r <kscdistr> <administrator>@<ksclinux.example.com>:
```

wobei:

`<kscdistr>` ist das lokale Verzeichnis mit den heruntergeladenen Programmpaketen von Kaspersky Security Center.

`<administrator>` ist ein Superuser auf dem neuen Administrationsserver, der zur Verwendung einer SSH-Verbindung berechtigt ist.

`<ksclinux.example.com>` ist die FQDN-Adresse des neuen Administrationsservers.

Die Dateien werden in die oberste Ebene des Home-Verzeichnisses des angegebenen Benutzers kopiert.

4. Konfigurieren der Installationseinstellungen

1. Melden Sie sich auf dem Gerät des neuen Administrationsservers als Superuser an und öffnen Sie ein Terminal.
2. Wechseln Sie in das Verzeichnis mit den kopierten Programmpaketen.

Beispiel

```
cd ~/kscdistr
```

3. Entpacken Sie das Archiv des Skripts für die Schnellinstallation in das aktuelle Verzeichnis mit den Distributionsdateien.

Beispiel

```
tar -xf ./ksc_fast_install.tar.gz
```

4. Überprüfen Sie durch Ausführen des folgenden Befehls, ob alle Dateien vorhanden sind:

```
ls -la
```

Beispiel für die Ausgabe des Befehls ls -la

```
administrator@ksclinux:~$ ls -la
drwxr-xr-x  3 administrator administrator      4096 jul 17 20:32 .
drwx------ 17 administrator administrator      4096 jul 17 17:54 ..
-rw-r--r--  1 administrator administrator       493 apr 20  2023 kaspersky_astra_pub_key.gpg
-rw-r--r--  1 administrator administrator 199128488 jul 10 21:38 ksc64_16.3.0-1207_amd64.deb
-rwxr-xr--  1 administrator administrator    143288 jul 22 17:22 ksc_fast_install.py
-rw-r--r--  1 administrator administrator 158144492 jul 10 21:37 ksc-web-console-16.3.12907.x86_64.deb
-rw-r--r--  1 administrator administrator     15561 jul 22 23:17 nwc_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 nwc_license.txt.sha256
-rw-r--r--  1 administrator administrator       493 jul 22 17:22 params.txt
-rw-r--r--  1 administrator administrator     70869 jul 22 23:17 server_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 server_license.txt.sha256
```

5. Öffnen Sie im Verzeichnis mit den Distributionsdateien die Textdatei mit den Einstellungen des Installationsskripts zum Bearbeiten, zum Beispiel:

```
nano ./params.txt
```

6. Legen Sie die zuvor vorbereiteten Werte fest und entfernen Sie das erste Kommentarzeichen (#) in den entsprechenden Zeilen, oder fügen Sie neue Zeilen mit den folgenden Werten hinzu:

   - Dimensionierung der Hardware (Werte für die Konfigurationen S/M/L/XL).

     Beispiel

     ```
     klfi_netsize=S
     ```

   - FQDN-Adresse des Administrationsservers in zwei Einstellungen in der Datei.

     ```
     klfi_klserver_address=ksclinux.example.com
     ```

     ```
     klfi_kliam_address=ksclinux.example.com
     ```

   Die Sprache des installierten Administrationsservers hängt vom Gebietsschema des heruntergeladenen Programmpakets ab.

7. Überprüfen Sie, ob der FQDN des Administrationsservers im Betriebssystem des neuen Administrationsservers korrekt in die Loopback-IP-Adresse aufgelöst wird. Gehen Sie dazu folgendermaßen vor:

   a. Führen Sie den Befehl `ping` mit der Adresse des neuen Administrationsservers aus.

   Beispiel für das erfolgreiche Abrufen einer Loopback-IP-Adresse

   ```
   administrator@ksclinux:~$ ping ksclinux.example.com
   ping ksclinux.example.com
   PING ksclinux.example.com (127.0.1.1) 56(84) bytes of data.
   64 bytes from ksclinux.example.com (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
   ```

b. Fügen Sie die Adresse des Administrationsservers der Datei `/etc/hosts` des Betriebssystems auf dem neuen Administrationsserver hinzu, wenn keine Adresse ermittelt wurde oder eine externe IP-Adresse ermittelt wurde.

   Gehen Sie dazu folgendermaßen vor:

   - Öffnen Sie die Datei `/etc/hosts` zur Bearbeitung, indem Sie den folgenden Befehl ausführen:

     ```
     sudo nano /etc/hosts
     ```

   - Geben Sie die Serveradresse als FQDN des Geräts des Administrationsservers ein, zum Beispiel:

     ```
     127.0.0.1       localhost
     127.0.1.1       ksclinux.example.com ksclinux
     <...>
     ```

> Auf verwalteten Geräten muss der FQDN des Administrationsservers in die externe IP-Adresse des Servers aufgelöst werden. Stellen Sie sicher, dass die Einträge auf den DNS-Servern korrekt eingerichtet sind.

5. Starten des Skripts für die Schnellinstallation

So führen Sie das Skript für die Schnellinstallation aus:

1. Wechseln Sie nach dem Neustart des Geräts wieder in das Verzeichnis mit den Programmpaketen:

   ```
   cd ~/kscdistr
   ```

2. Machen Sie die Datei ausführbar, indem Sie den folgenden Befehl ausführen:

   ```
   chmod +x ./ksc_fast_install.py
   ```

3. Lesen Sie die Endbenutzer-Lizenzverträge in Ihrer Lokalisierungssprache, bevor Sie das Skript ausführen, da das Skript für die Schnellinstallation selbst nur auf Englisch verfügbar ist.

4. Binden Sie die Netzwerk-Paket-Repositorys in das Betriebssystem oder das Installationsdatenträgerabbild des Betriebssystems ein, damit Pakete während der Installation heruntergeladen werden können.

5. Führen Sie das Skript für die Schnellinstallation aus:

   ```
   sudo ./ksc_fast_install.py
   ```

6. Befolgen Sie die Schritte des Installationsassistenten.

> Wenn das Skript im Schritt der Ressourcenprüfung fälschlicherweise meldet, dass nicht genügend RAM vorhanden ist, deaktivieren Sie während der Installation die dynamische RAM-Zuweisung.

7. Warten Sie, bis die Installation abgeschlossen ist. Speichern Sie aus der Textausgabe des Skripts den Benutzernamen (`User`) und das Kennwort (`Pass`) für die Web Console.

Beispiel

```
[+] Creating KSC user 'kscadmin' ...
[+] An internal user has been created:
[+]     User: kscadmin
[+]     Pass: ############
[!] If the password is lost, you must create a user by running the command:
        /opt/kaspersky/ksc64/sbin/kladduser -n <user>
[+] OK
[+] Success
```

Video: Ausführen des Schnellinstallationsskripts für Ubuntu



6. Erstmalige Anmeldung bei der Web Console

1. Öffnen Sie in einem Browser die Adresse der Web Console: `https://<FQDN>:8080`

   wobei `<FQDN>` die Adresse des Administrationsservers aus den Einstellungen des Installationsskripts ist, z. B. *https://ksclinux.example.com:8080*.

2. Melden Sie sich mit dem Benutzernamen und dem Kennwort aus der Skriptausgabe bei der Web Console an.

3. Konfigurieren Sie die Authentifikator-App:

   a. Kopieren Sie den geheimen Schlüssel zum Abrufen einmaliger Bestätigungscodes in die Anwendung oder scannen Sie den QR-Code aus dem Authentifizierungsassistenten der Web Console.

   b. Geben Sie den generierten Bestätigungscode ein, um sich zu authentifizieren und bei der Web Console anzumelden.

4. Lesen und bestätigen Sie den Leitfaden zur Härtung.

5. Konfigurieren Sie den Administrationsserver im Assistent für die Ersteinrichtung, wenn Sie nicht vorhaben, die Daten des Administrationsservers aus einer Backup-Kopie wiederherzustellen.

4 Wiederherstellen einer Backup-Kopie des Administrationsservers

In Szenarien der Migration von Kaspersky Security Center Windows oder der Migration von Daten aus Kaspersky Security Center Linux auf neue Hardware müssen Sie möglicherweise Daten aus einer Backup-Kopie wiederherstellen, die in der alten Installation des Administrationsservers erstellt wurde.

Die PostgreSQL-Version auf dem neuen Server muss mindestens der Version in der Backup-Kopie entsprechen.

Überspringen Sie diesen Schritt, wenn Sie keine Daten wiederherstellen müssen.

Wenn zuvor keine Backup-Kopie erstellt wurde:

- Erstellen Sie eine Backup-Kopie der alten Installation des Administrationsservers mit dem Datenformattyp PostgreSQL.
- Installieren Sie einen neuen Server für Kaspersky Security Center Linux und melden Sie sich zum ersten Mal bei der Web Console an.

Das Wiederherstellen des Administrationsservers aus einer Backup-Kopie umfasst die folgenden Schritte:

1. Ablegen der Backup-Kopie auf dem Administrationsserver

Legen Sie die Backup-Kopie des alten Administrationsservers mithilfe von Wechseldatenträgern oder über das Netzwerk auf dem neuen Gerät des Administrationsservers ab.

So kopieren Sie die Backup-Kopie über das Netzwerk auf den Administrationsserver:

Ob Sie das Dienstprogramm scp zum Kopieren der Dateien verwenden können, hängt davon ab, ob im Betriebssystem des Geräts des Administrationsservers ein SSH-Dienst ausgeführt wird, sowie von der Sicherheitsrichtlinie Ihrer Organisation.

1. Wechseln Sie in der Befehlszeile mit dem Befehl *cd* zu dem Verzeichnis, das die Backup-Dateien des vorherigen Administrationsservers enthält, zum Beispiel:

   Windows

   ```
   cd C:\kscbackups
   ```

   Linux

   ```
   cd /root/kscbackups
   ```

2. Kopieren Sie das Verzeichnis mit den Backup-Dateien mithilfe des Dienstprogramms scp:

   ```
   scp -r <klbackup202x-xx-xx> <administrator>@<ksclinux.example.com>:
   ```

   wobei:

   `<klbackup202x-xx-xx>` ist das Verzeichnis, in dem die Backup-Dateien gespeichert werden.

`<administrator>` ist ein Superuser auf dem neuen Administrationsserver, der zur Verwendung einer SSH-Verbindung berechtigt ist.

`<ksclinux.example.com>` ist die FQDN-Adresse des neuen Administrationsservers.

Das Verzeichnis mit der Backup-Kopie wird in das Home-Verzeichnis des angegebenen Benutzers kopiert.

2. Verfahren zur Wiederherstellung aus einem Backup

1. Öffnen Sie auf dem neuen Gerät des Administrationsservers das Terminal.
2. Gewähren Sie während der Wiederherstellung von Daten aus einer Backup-Kopie den Standardkonten klserver und kliam, die der Administrationsserver für die Verbindung mit der Datenbank verwendet, PostgreSQL-Superuser-Rechte:

   ```
   sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
   ```

   ```
   sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
   ```

3. Verwenden Sie das Dienstprogramm klbackup, um die Datenwiederherstellung aus der Backup-Kopie des alten Administrationsservers zu starten:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klbackup -path </home/administrator/klbackup202x-xx-xx> -restore
   ```

   wobei `</home/administrator/klbackup202x-xx-xx>` für den vollständigen Pfad zum Verzeichnis mit den Backup-Dateien steht.

4. Wenn für das Backup kein Kennwort festgelegt wurde, drücken Sie bei der Aufforderung zur Eingabe eines Kennworts für das Backup die **Eingabetaste**, ohne ein Kennwort einzugeben.
5. Warten Sie, bis das Dienstprogramm beendet ist.

   Große Installationen können sehr lange dauern.

6. Stellen Sie die ursprünglichen Berechtigungen für die PostgreSQL-Benutzerkonten wieder her, die der Administrationsserver für die Verbindung mit der Datenbank verwendet.

   ```
   sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
   ```

   ```
   sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
   ```

5 Konfigurieren des Programms nach der Wiederherstellung aus einer Backup-Kopie

Überspringen Sie diesen Schritt, wenn Sie keine Daten aus einer Backup-Kopie wiederhergestellt haben.

Das Konfigurieren des Programms nach der Wiederherstellung aus einer Backup-Kopie umfasst die folgenden Schritte:

1. Wiederherstellen der Web Console

1. Rufen Sie die Adresse des alten Servers aus der Konfigurationsdatei des IAM-Servers ab:

```
sudo grep "ksc_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Beispiel

```
ksc_address: "oldksc.example.internal"
```

2. Überprüfen Sie, ob der FQDN des alten Administrationsservers korrekt in die Loopback-IP-Adresse des neuen Administrationsservers aufgelöst wird. Gehen Sie dazu folgendermaßen vor:

   a. Führen Sie den Befehl `ping` mit der Adresse des alten Administrationsservers aus.

Beispiel für das erfolgreiche Abrufen einer Loopback-IP-Adresse

```
administrator@ksclinux:~$ ping oldksc.example.internal
ping oldksc.example.internal
PING ksclinux (127.0.1.1) 56(84) bytes of data.
64 bytes from ksclinux (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
```

   b. Fügen Sie die Adresse des Administrationsservers der Datei `/etc/hosts` des Betriebssystems auf dem neuen Administrationsserver hinzu, wenn keine Adresse ermittelt wurde oder eine externe IP-Adresse ermittelt wurde. Gehen Sie dazu folgendermaßen vor:

   - Öffnen Sie die Datei /etc/hosts zum Bearbeiten:

```
sudo nano /etc/hosts
```

   - Geben Sie den Namen des alten Servers als zusätzlichen Alias für die Adresse des Geräts des Administrationsservers ein.

Beispiel

```
127.0.0.1       localhost
127.0.1.1       ksclinux.example.com ksclinux oldksc.example.internal
<...>
```

3. Installieren Sie die Web Console neu:

   a. Deinstallieren Sie den lokalen Server der Web Console:

   Führen Sie je nach Programmpaket für Kaspersky Security Center Linux einen der folgenden Befehle aus:

   - Auf einem Debian-basierten Betriebssystem:

```
sudo apt remove ksc-web-console -y
```

   - Auf einem Gerät mit einem auf Red Hat Enterprise Linux basierenden Betriebssystem:

```
sudo dnf remove ksc-web-console -y
```

b. Installieren Sie das Web Console-Paket aus dem Verzeichnis mit den Programmpaketen:

- Auf einem Debian-basierten Betriebssystem:

```
sudo apt install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.deb -y
```

- Auf einem Gerät mit einem auf Red Hat Enterprise Linux basierenden Betriebssystem:

```
sudo dnf install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.rpm -y
```

2. Wiederherstellen des Zugriffs des Benutzers kscadmin bei der Migration von Kaspersky Security Center Windows

Die Benutzerdatenbank wurde überschrieben; erstellen Sie den Benutzer kscadmin neu und konfigurieren Sie die Zwei-Faktor-Authentifizierung.

1. Öffnen Sie das Terminal im Betriebssystem des Geräts des Administrationsservers und führen Sie den folgenden Befehl aus, um einen Benutzer zu erstellen:

   ```
   sudo /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin
   ```

   Nachdem Sie die **Eingabetaste** gedrückt haben, geben Sie ein Kennwort ein und geben Sie es anschließend erneut ein.

2. Öffnen Sie in einem Browser die Adresse der Web Console:

   ```
   https://<FQDN>:8080
   ```

   wobei `<FQDN>` die Adresse des Administrationsservers aus den Einstellungen des Installationsskripts ist, z. B. *https://ksclinux.example.com:8080*.

3. Verwenden Sie den erstellten Benutzernamen und das Kennwort, um sich bei der Web Console anzumelden.

4. Konfigurieren Sie die Authentifikator-Anwendung. Gehen Sie dazu folgendermaßen vor:

   a. Löschen Sie das alte Benutzerprofil des Benutzers kscadmin aus der Authentifikator-Anwendung, bevor Sie die Backup-Kopie des Administrationsservers wiederherstellen.

   b. Kopieren Sie den geheimen Schlüssel zum Abrufen einmaliger Bestätigungscodes in die Anwendung oder scannen Sie den QR-Code aus dem Authentifizierungsassistenten der Web Console.

   c. Geben Sie den generierten Bestätigungscode ein, um sich zu authentifizieren und bei der Web Console anzumelden.

3. Testen des Administrationsservers

1. Überprüfen Sie, ob die Benutzeroberfläche der Web Console bei der Anmeldung als kscadmin und als andere Benutzer ordnungsgemäß funktioniert.

2. Führen Sie nacheinander die folgenden Aufgaben aus:

   - Updates in die Datenverwaltung des Administrationsservers herunterladen
   - Wartung des Administrationsservers
   - Datensicherung des Administrationsservers

   > Ersetzen Sie die Windows-Pfade in den Aufgabeneinstellungen durch Linux-Verzeichnisse auf dem neuen Administrationsserver oder löschen Sie die Aufgaben und konfigurieren Sie sie von Grund auf neu.

3. Überprüfen Sie die Ergebnisse der Aufgaben und nehmen Sie gegebenenfalls Änderungen an den Aufgabeneinstellungen, den Verwaltungsrichtlinien und den Einstellungen des Administrationsservers vor.

4. Wiederherstellen der Verbindung verwalteter Geräte zum FQDN des vorherigen Administrationsservers

Wenn Sie dem neuen Administrationsserver einen neuen FQDN zugewiesen haben (z. B. ksclinux.example.com), fügen Sie einen der folgenden Typen von DNS-Einträgen hinzu:

- Ein CNAME-Eintrag, der den alten Namen des Administrationsservers dem neuen Namen des Administrationsservers zuordnet.

  Einzelheiten zur Konfiguration der erforderlichen Einträge finden Sie in der Dokumentation Ihres DNS-Servers.

- A- und AAAA-Einträge für die vorherige Adresse des Administrationsservers, die auf die neue IP-Adresse des Administrationsservers verweisen.

  Führen Sie für einen DNS-Dienst auf Basis von Windows Server die Befehle mit den für Ihre Infrastruktur geltenden Werten aus.

Um einem DNS-Dienst auf Basis von Windows Server einen DNS-A-Eintrag hinzuzufügen, führen Sie die Befehle mit den für Ihre Infrastruktur geltenden Werten aus:

1. Stellen Sie eine Verbindung mit Ihrem DNS-Server her.

2. Öffnen Sie PowerShell und rufen Sie die IP-Adresse aus dem vorhandenen A-Eintrag ab, indem Sie den folgenden Befehl ausführen:

   ```
   Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
   ```

3. Ändern Sie die IP-Adresse im A-Eintrag, indem Sie die folgenden Befehle ausführen:

```
$OldKSC = Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

```
$NewKSC = $OldKSC.Clone()
```

```
$NewKSC.RecordData.IPv4Address = [System.Net.IPAddress]::parse('<IP-address of the administration server>')
```

```
Set-DnsServerResourceRecord -OldInputObject $OldKSC -NewInputObject $NewKSC -ZoneName "<zone name>"
```

4. Überprüfen Sie, ob die IP-Adresse im A-Eintrag aktualisiert wurde, indem Sie den folgenden Befehl ausführen:

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

Die Ausgabe des Befehls enthält die IP-Adresse des Administrationsservers von Kaspersky Security Center Linux. Verwaltete Geräte stellen die Verbindung wieder her, nachdem der lokale DNS-Cache aktualisiert wurde.

6 Konfigurieren des Antiviren-Schutzes des Administrationsservers

Um die Empfehlungen des Hardening Guides zur Bereitstellung des Antiviren-Schutzes für den Administrationsserver einzuhalten, installieren Sie Kaspersky-Programme auf dem Administrationsserver und konfigurieren Sie Verwaltungsrichtlinien. Informationen zur Bereitstellung von Kaspersky Endpoint Security für Linux finden Sie im Bereitstellungshandbuch.

Die Installation und Konfiguration bestehen aus den folgenden Schritten:

1. Erstellen einer separaten Administrationsgruppe

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Gruppenhierarchie** aus.
2. Aktivieren Sie das Kontrollkästchen neben der Gruppe **Verwaltete Geräte**.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**.
4. Geben Sie im angezeigten Fenster einen Namen für die neue Gruppe an (z. B. *kscserver*) und bestätigen Sie die Erstellung durch Klicken auf die Schaltfläche **Hinzufügen**.

2. Erstellen einer Richtlinie für den Administrationsagenten ohne Vererbung von Einstellungen

1. Wechseln Sie im Hauptfenster der Web Console zum Abschnitt **Geräteverwaltung** → **Richtlinien**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie im Assistent für das Erstellen einer Richtlinie das Programm **Kaspersky Security Center Administrationsagent** aus und klicken Sie auf **Weiter**.
4. Deaktivieren Sie die Option **Einstellungen von übergeordneter Richtlinie erben** und klicken Sie auf **Speichern**.

3. Installieren des Verwaltungs-Plug-ins für Kaspersky Endpoint Security für Linux über Kaspersky Security Center oder manuell

Sie können das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Linux auf folgende Arten installieren:

- Installation aus der Liste der verfügbaren Programmpakete in der Web Console.
- Manuelle Installation aus einer Datei.

So installieren Sie das Verwaltungs-Plug-in für Kaspersky Endpoint Security aus der Liste der verfügbaren Programmpakete in der Web Console:

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

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

2. Klicken Sie auf **Hinzufügen**.

   Dadurch wird die Liste der verfügbaren Verwaltungs-Plug-ins geöffnet. Die Liste wird automatisch aktualisiert, wenn neue Versionen der Web-Plug-ins veröffentlicht werden.

3. Wählen Sie in der Liste der verfügbaren Plug-ins die neueste verfügbare Version des Web-Plug-ins für Kaspersky Endpoint Security für Linux aus.

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

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

Das neue Plug-in wird in der Liste der installierten Web-Plug-ins angezeigt.

Video: Installation des Verwaltungs-Web-Plug-ins mithilfe des Assistenten



So installieren Sie das Verwaltungs-Plug-in für Kaspersky Endpoint Security manuell aus einer Datei:

1. Laden Sie das Archiv mit dem Web-Plug-in von der Downloadseite des Programms im Abschnitt Kaspersky Endpoint Security für Linux herunter: **Programmkontrolle-Plug-in** → **Web Console-Plug-in**.

2. Entpacken Sie das heruntergeladene Archiv lokal.

3. Wählen Sie im Hauptfenster der Web Console **Einstellungen** → **Web-Plug-ins** aus.

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

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

5. Daraufhin wird ein Fenster geöffnet. Geben Sie in diesem Fenster den Pfad zur Datei plugin.zip und den Pfad zur Datei signature.txt an.

   Die Dateien befinden sich in dem Ordner, in den Sie das Archiv mit dem Web-Plug-in entpackt haben.

6. Klicken Sie auf **Hinzufügen**.

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

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

Video: Installation des Verwaltungs-Web-Plug-ins in isolierten Netzwerken



4. Erstellen einer Richtlinie für Kaspersky Endpoint Security für Linux ohne Vererbung der Einstellungen

Wenn Sie Kaspersky Endpoint Security für Linux zusammen mit Kaspersky Security Center Linux verwenden, müssen Sie die Richtlinieneinstellungen gemäß den Empfehlungen von Kaspersky-Experten verwalten.

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Wählen Sie eine Administrationsgruppe für den Administrationsserver aus.

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

   Der Assistent für neue Richtlinien wird gestartet.

4. Wählen Sie im angezeigten Fenster Kaspersky Endpoint Security für Linux aus der Liste aus.

5. Geben Sie **Standard-Modus oder Endpoint Detection and Response Agent-Modus** des Programms Kaspersky Endpoint Security für Linux an.

6. Entscheidung Sie sich über die Verwendung von Kaspersky Security Network.

7. Lesen Sie die Optimierungsempfehlungen für verwaltete Geräte.

8. Geben Sie im Namen der Richtlinie an, dass die Richtlinie zum Administrationsserver gehört.

9. Deaktivieren Sie die Option **Einstellungen aus übergeordneter Richtlinie übernehmen**.

10. Speichern Sie die vorgenommenen Änderungen.

Video: Erstellen einer Richtlinie



5. Erstellen der Gruppenaufgabe „Update“ für Kaspersky Endpoint Security für Linux

1. Wählen Sie im Hauptfenster der Web Console den Abschnitt **Aufgaben** aus.

2. Wählen Sie eine Administrationsgruppe für den Administrationsserver aus.

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

   Der Assistent für neue Aufgaben wird gestartet.

4. Wählen Sie im angezeigten Fenster Kaspersky Endpoint Security für Linux aus der Liste aus.

5. Geben Sie als Aufgabentyp *Update* an und führen Sie die nächsten Schritte aus, ohne die Einstellungen zu ändern.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

6. Aktivieren Sie im Abschnitt **Anwendungseinstellungen** → **Update-Quellen** die Quelle Kaspersky Security Center und erhöhen Sie ihre Priorität.

Verwenden Sie in einem isolierten Netzwerk das Kaspersky Update Utility, um ein Repository für Update-Aufgaben zu erstellen.

Video: Konfigurieren zentralisierter Datenbanken-Updates



6. Hinzufügen eines Lizenzschlüssels zum Speicher des Administrationsservers mit Funktion zur automatischen Schlüsselverteilung

1. Wechseln Sie im Hauptfenster von Kaspersky Security Center Web Console zum Abschnitt **Lizenzen**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Wählen Sie die Option **Aktivierungscode** aus und klicken Sie auf **Senden**.

   Verwenden Sie in einem isolierten Netzwerk eine Schlüsseldatei, die Sie über den Dienst https://keyfile.kaspersky.com/de-DE anfordern können.
4. Klicken Sie in der Liste der Lizenzen auf den Namen der Lizenz.
5. Aktivieren Sie das Kontrollkästchen **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.
6. Speichern Sie die vorgenommenen Änderungen.

Video: Aktivierung des Programms mit einem Aktivierungscode



Video: Aktivierung des Programms mit einer Schlüsseldatei



7. Erstellen von Installationspaketen für den Administrationsagenten und Kaspersky Endpoint Security für Linux

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Software-Verwaltung** → **Installationspakete** aus.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen eines Installationspakets wird gestartet.
3. Wählen Sie den Punkt **Installationspaket für eine Kaspersky-Anwendung erstellen**.
4. Suchen Sie in der Liste der Programme nach der neuesten Version von Kaspersky Endpoint Security für Linux und klicken Sie auf den Namen.
5. Starten Sie den Download in der Seitenleiste, indem Sie auf die Schaltfläche **Herunterladen und Installationspaket erstellen** klicken.

   Lesen und akzeptieren Sie die Endbenutzer-Lizenzverträge, um die Programme zu verwenden.
6. Kehren Sie zur Liste der Programme zurück und laden Sie die neueste Version des Administrationsagenten für Linux herunter.

   Lesen und akzeptieren Sie die Endbenutzer-Lizenzverträge, um die Programme zu verwenden.
7. Klicken Sie im Hauptfenster der Web Console in der Liste der heruntergeladenen Programme auf die Namen der Programme.

Laden Sie in einem isolierten Netzwerk die Programmpakete von der Kaspersky-Website herunter und wählen Sie im Assistenten für das Erstellen eines Installationspakets die Option **Installationspaket aus einer Datei erstellen** aus.

Video: Automatische Erstellung eines Installationspakets in Kaspersky Security Center



Video: Manuelles Erstellen eines Installationspakets in Kaspersky Security Center



8. Installation des Administrationsagenten für Linux

1. Wählen Sie im Hauptfenster von Web Console **Softwareverwaltung** → **Installationspakete** aus.
2. Aktivieren Sie das Kontrollkästchen neben dem Paket **Kaspersky Administrationsagent für Linux**.
3. Klicken Sie auf **Erweitern**.

   Der Softwareverteilungs-Assistent wird gestartet.
4. Wählen Sie die Option **Autonomes Paket verwenden** aus.
5. Überspringen Sie im Schritt **Geräte in den Ordner „Verwaltete Geräte“ verschieben** die Konfiguration von Regeln zum Verschieben von Geräten in eine Administrationsgruppe. Diese Option gilt nicht für das Gerät mit dem Administrationsserver.
6. Wählen und kopieren Sie im Schritt **Ergebnis der Erstellung des autonomen Installationspakets** den vollständigen Pfad zum Installationsskript des Programms.
7. Öffnen Sie im Betriebssystem des Administrationsservers die Befehlszeile.

8. Starten Sie die Installation des autonomen Pakets:

```
sudo bash "</var/opt/.../stand-alone_package_sh>"
```

wobei `</var/opt/.../stand-alone_package_sh>` der zuvor kopierte vollständige Pfad zur Skriptdatei des autonomen Installationspakets des Programms ist.

Wenn die Installation erfolgreich war, wird eine entsprechende Benachrichtigung angezeigt.

9. Verschieben Sie das Gerät mit dem Administrationsserver (z. B. *ksclinux*) aus der Gruppe **Verwaltete Geräte** in eine zuvor vorbereitete Administrationsgruppe (z. B. *kscserver*).

9. Installation von Kaspersky Endpoint Security für Linux

1. Wählen Sie im Hauptfenster von Web Console **Softwareverwaltung** → **Installationspakete** aus.
2. Aktivieren Sie das Kontrollkästchen neben dem Paket Kaspersky Endpoint Security für Linux.
3. Klicken Sie auf **Erweitern**.

   Der Softwareverteilungs-Assistent wird gestartet.
4. Wählen Sie die Option **Autonomes Paket verwenden** aus.
5. Wählen und kopieren Sie im Schritt **Ergebnis der Erstellung des autonomen Installationspakets** den vollständigen Pfad zum Installationsskript des Programms.
6. Öffnen Sie im Betriebssystem des Administrationsservers die Befehlszeile.
7. Starten Sie die Installation des autonomen Pakets:

```
sudo bash "</var/opt/.../stand-alone_package_sh>"
```

wobei `</var/opt/.../stand-alone_package_sh>` der zuvor kopierte vollständige Pfad zur Skriptdatei des autonomen Installationspakets des Programms ist.

Wenn die Installation erfolgreich war, wird eine entsprechende Benachrichtigung angezeigt.

8. Wählen Sie im Hauptfenster von Web Console im Abschnitt **Aufgaben** in der Liste der Administrationsgruppen den Stammknoten mit dem Namen des Administrationsservers aus.
9. Starten Sie aus der Liste der Aufgaben des Administrationsservers nacheinander die folgenden Aufgaben:
   - Updates in die Datenverwaltung des Administrationsservers herunterladen
   - Update (Kaspersky Endpoint Security für Linux)
10. Wählen Sie im Hauptfenster der Web Console **Asset-Management** → **Assets (Geräte)** aus.
11. Klicken Sie auf den Namen des Geräteobjekts des Administrationsservers.
12. Überprüfen Sie die Hauptindikatoren des Gerätestatus:
    - Das letzte Update der Antiviren-Datenbanken (aktuell).
    - Mit dem Administrationsserver verbunden (aktuell).

- Schutzstatus (Wird ausgeführt).
- *Schlüssel erfolgreich hinzugefügt*-Ereignis (vorhanden).

Verwenden Sie das Bereitstellungshandbuch für Kaspersky Endpoint Security für Linux, um die Sicherheitslösung auf Geräten in Ihrem Netzwerk bereitzustellen.

Update einer Vorgängerversion der Anwendung durchführen

Das Programm Kaspersky Endpoint Security kann aktualisiert werden, indem eine neue Version des Programms per Fernzugriff oder lokal auf den geschützten Geräten installiert wird.

Ein Upgrade auf Kaspersky Endpoint Security 12.5 für Linux ist nur für die Version Kaspersky Endpoint Security 12.4 für Linux möglich.

Es ist nicht möglich, Kaspersky Endpoint Security von früheren Versionen auf Version 12.5 zu aktualisieren. Wenn Sie eine frühere Version von Kaspersky Endpoint Security installiert haben, müssen Sie diese zunächst deinstallieren und anschließend Kaspersky Endpoint Security 12.5 für Linux installieren.

Sie können diese Schritte ausführen, um das Programm zu aktualisieren.

1 Umgebung vorbereiten

Führen Sie vor dem Upgrade von Kaspersky Endpoint Security die erforderlichen vorbereitenden Schritte aus, die von Ihrer Infrastruktur abhängen.

2 Programmpakete vorbereiten

Wählen Sie ein Distributionspaket aus, abhängig von Ihrem Betriebssystem, seiner Architektur und dem CPU-Typ.

3 Aktualisieren des Verwaltungs-Plug-ins für Kaspersky Endpoint Security

Wenn Sie Kaspersky Endpoint Security mithilfe von Kaspersky Security Center verwalten, aktualisieren Sie je nach Konsole, die Sie zur Verwaltung von Kaspersky Security Center verwenden, das Web-Plug-in oder das MMC-Plug-in zur Verwaltung von Kaspersky Endpoint Security.

4 Aktualisieren der Anwendung und der grafischen Oberfläche auf geschützten Geräten

Installieren Sie die neue Version des Programms auf Ihren geschützten Geräten. Die aktualisierte Anwendung übernimmt den Nutzungsmodus, der bei der Installation ausgewählt wurde. Wenn Sie die Anwendung in einem anderen Modus verwenden möchten, müssen Sie die Anwendung zunächst deinstallieren und anschließend die Installationsprozedur und die Konfiguration zur Erstkonfiguration der Anwendung durchführen.

Wenn Sie Kaspersky Endpoint Security im Basismodus oder im EDR-Agent-Modus verwenden und die grafische Benutzeroberfläche des Programms nutzen, aktualisieren Sie auch die grafische Benutzeroberfläche.

Sie können die Anwendung und die grafische Oberfläche der Anwendung auf folgende Weise aktualisieren:

- Remote mittels Kaspersky Security Center
- Lokal über die Befehlszeile

So aktualisieren Sie das Programm aus einem RPM-Paket mithilfe der Befehlszeile

Das Upgrade des Programms über die Befehlszeile entspricht der Installation einer neuen Version des Programms auf dem Gerät.

Sie benötigen Root-Rechte, um das Programm zu aktualisieren.

Um das Programm zu aktualisieren, führen Sie den folgenden Befehl aus:

```
# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=<yes|no>] rpm -U --replacefiles --
replacepkgs kesl-12.5.0-<build number>.<arch>.rpm [kesl-gui-12.5.0-<build number>.<arch>.rpm]
```

Kaspersky Endpoint Security wird automatisch neu gestartet.

Symbole

Befehlsoptionen

Parameter	Description
`KESL_EULA_AGREED=yes`	Akzeptieren Sie die Bedingungen des Endbenutzer-Lizenzvertrags.
`KESL_PRIVACY_POLICY_AGREED=yes`	Akzeptieren Sie die Bedingungen der Datenschutzrichtlinie.
`KESL_USE_KSN=yes/no`	Verwenden von Kaspersky Security Network: `yes` – die Bedingungen der Erklärung zu Kaspersky Security Network akzeptieren und die Verwendung von Kaspersky Security Network aktivieren. `no` – die Bedingungen der Erklärung zu Kaspersky Security Network ablehnen und die Verwendung von Kaspersky Security Network deaktivieren.
`<arch>`	Architekturtyp: `i386` – für 32-Bit-Betriebssysteme `x86_64` – für 64-Bit-Betriebssysteme `aarch64` – für 64-Bit-Betriebssysteme für die Arm-Architektur

Kaspersky Endpoint Security wird automatisch neu gestartet.

Beispiel:

Aktualisieren Sie das RPM-Anwendungspaket mit dem GUI-Paket für 64-Bit-Betriebssysteme:

```
# KESL_EULA_AGREED=yes KESL_PRIVACY_POLICY_AGREED=yes KESL_USE_KSN=yes rpm -U --replacefiles --replacepkgs kesl-12.5.0-<build number>.x86_64.rpm kesl-gui-12.5.0-<build number>.x86_64.rpm
```

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

So aktualisieren Sie das Programm aus einem DEB-Paket mithilfe der Befehlszeile

Das Upgrade des Programms über die Befehlszeile entspricht der Installation einer neuen Version des Programms auf dem Gerät.

Sie benötigen Root-Rechte, um das Programm zu aktualisieren.

Um das Programm zu aktualisieren, führen Sie den folgenden Befehl aus:

```
# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=<yes|no>] apt-get install ./kesl_12.5.0-<build number>_<arch>.deb [./kesl-gui_12.5.0-<build number>_<arch>.deb]
```

Kaspersky Endpoint Security wird automatisch neu gestartet.

Symbole

Befehlsoptionen

Parameter	Description
`KESL_EULA_AGREED=yes`	Akzeptieren Sie die Bedingungen des Endbenutzer-Lizenzvertrags.
`KESL_PRIVACY_POLICY_AGREED=yes`	Akzeptieren Sie die Bedingungen der Datenschutzrichtlinie.
`KESL_USE_KSN=yes/no`	Verwenden von Kaspersky Security Network: `yes` – die Bedingungen der Erklärung zu Kaspersky Security Network akzeptieren und die Verwendung von Kaspersky Security Network aktivieren. `no` – die Bedingungen der Erklärung zu Kaspersky Security Network ablehnen und die Verwendung von Kaspersky Security Network deaktivieren.
`<arch>`	Architekturtyp: `i386` – für 32-Bit-Betriebssysteme `amd64` – für 64-Bit-Betriebssysteme `arm64` – für 64-Bit-Betriebssysteme für die Arm-Architektur

Beispiel:

Aktualisieren Sie das DEB-Anwendungspaket mit dem GUI-Paket für 64-Bit-Betriebssysteme:

```
# KESL_EULA_AGREED=yes KESL_PRIVACY_POLICY_AGREED=yes KESL_USE_KSN=yes apt-get install ./kesl_12.5.0-<build number>_amd64.deb [./kesl-gui_12.5.0-<build number>_amd64.deb]
```

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

5 Aktualisieren des Kaspersky Security Center Administrationsagenten

Optionaler Schritt. Wenn Sie Kaspersky Endpoint Security zentral mithilfe von Kaspersky Security Center verwalten, aktualisieren Sie den Administrationsagenten auf den geschützten Geräten. Das Upgrade wird durch Installation einer neuen Version des Administrationsagenten durchgeführt.

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

Während des Updates des Administrationsagenten funktioniert die App weiterhin ordnungsgemäß.

Besonderheiten des Upgrades einer älteren Programmversion

- 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.

- Wenn Sie auf einem Betriebssystem mit einem Paketmanager des Typs `rpm` das Anwendungspaket zusammen mit dem GUI-Paket installiert haben, wird es nicht empfohlen, nur eines der Pakete zu aktualisieren.

  Wenn Sie auf einem Betriebssystem mit einem Paketmanager des Typs `dpkg` das Anwendungspaket zusammen mit dem GUI-Paket installiert haben, ist es nicht möglich, eines der Pakete ohne das andere zu aktualisieren.

- Wenn sich in der neuen Version des Programms die Bedingungen des Endbenutzer-Lizenzvertrags und/oder der Datenschutzrichtlinie geändert haben, müssen Sie während des Updates die neuen Bedingungen akzeptieren. Die Texte der Benutzervereinbarungen sind auf der Kaspersky-Website (im Abschnitt **EULA**) sowie im Verzeichnis `~/.kesl/12.5/license.<language ID>` verfügbar.

  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 Anwendung geändert haben, müssen Sie die neuen Bedingungen für Verwendung von Kaspersky Security Network akzeptieren oder ablehnen. Der Text der Erklärung zu Kaspersky Security Network ist unter ~/.kesl/12.5/ksn_license.<language ID> verfügbar. Wenn Sie die Verwendung von Kaspersky Security Network ablehnen, wird der Update-Vorgang nicht unterbrochen. Sie können den Modus von Kaspersky Security Network später aktivieren, deaktivieren oder ändern.

  Wenn Sie in einer Vorgängerversion des Programms KSN verwendet und die Bedingungen der Erklärung zu Kaspersky Security Network akzeptiert haben, müssen Sie beim Update des Programms die Bedingungen der Erklärung zu Kaspersky Security Network akzeptieren. Andernfalls wird die Verwendung von KSN deaktiviert.

- 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 Anwendung aktualisieren, werden die Dump-Dateien vorheriger Versionen gelöscht.

- Beim Update des Programms wird die Ereignisprotokolldatei der Vorgängerversion zur ersten Ereignisdatei im Dateisatz der aktuellen Version. Diese Datei wird gespeichert, bis die Anzahl der Ereignisse in den verbleibenden Dateien die angegebene maximale Anzahl erreicht (mittels Parameter `MaxEventsNumber`). Daher kann es vorübergehend vorkommen, dass die Anwendung doppelt so viele Ereignisse speichert, wie durch den Parameter `MaxEventsNumber` festgelegt.

- Wenn Kaspersky Endpoint Security im Basismodus oder im EDR-Agent-Modus verwendet wird, empfehlen wir, nach dem Update des Programms die Aufgabe Datenbanken-Update zu starten.

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.

So installieren Sie das Verwaltungs-Web-Plug-in

Sie können das Web-Plug-in folgendermaßen installieren:

- 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 Erstkonfiguration auszuführen. Sie können den Assistenten für die Erstkonfiguration auch in der Oberfläche 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 Schnellstartassistenten für Kaspersky Security Center Web Console finden Sie in der Hilfe zu Kaspersky Security Center.

- Manuell mithilfe eines Programmpakets aus der Liste der Kaspersky-Web-Plug-ins oder aus einer Datei.

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

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. Klicken Sie auf **Hinzufügen**.

   Dadurch wird die Liste der verfügbaren Verwaltungs-Plug-ins geöffnet. Die Liste wird automatisch aktualisiert, wenn neue Versionen der Web-Plug-ins veröffentlicht werden.

3. Wählen Sie in der Liste der verfügbaren Plug-ins das Web-Plug-in **Kaspersky Endpoint Security <Versionsnummer> für Linux** aus.

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

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

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

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

1. Laden Sie das Archiv mit dem Web-Plug-in von der Downloadseite des Programms im Abschnitt **Kaspersky Endpoint Security für Linux** herunter (**Zusätzliches Distributionspaket** → **Web Console-Plug-in**).

2. Entpacken Sie das heruntergeladene Archiv lokal.

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

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

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

5. Daraufhin wird ein Fenster geöffnet. Geben Sie in diesem Fenster den Pfad zur Datei plugin.zip und den Pfad zur Datei signature.txt an. Die Dateien befinden sich in dem Ordner, in den Sie das Archiv mit dem Web-Plug-in entpackt haben.

6. Klicken Sie auf **Hinzufügen**.

7. 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 Anwendung Kaspersky Endpoint Security vorhanden ist, werden der Endbenutzer-Lizenzvertrag und die gesamte Oberfläche in der Kaspersky Security Center Web Console in englischer Sprache angezeigt.

So installieren Sie das MMC-Verwaltungs-Plug-in

Vor der Installation des MMC-basierten Verwaltungs-Plug-ins von 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:

1. Laden Sie die Datei klcfginst.msi von der Downloadseite des Programms im Abschnitt **Kaspersky Endpoint Security für Linux** herunter (**Build** → **Administrations-Plug-in**).

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

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

So zeigen Sie die Liste der installierten MMC-Plug-ins für die Verwaltung 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:

   - Öffnen Sie das Kontextmenü des Knotens **Administrationsserver <Servername>** und wählen Sie den Eintrag **Eigenschaften** aus.

   - Klicken Sie im Arbeitsbereich des Knotens **Administrationsserver <Servername>** im Abschnitt **Administrationsserver** auf den Link **Eigenschaften des Administrationsservers**.

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

Konvertierung von Richtlinien und Aufgaben

Richtlinien und Aufgaben, die für vorherige Versionen von Kaspersky Endpoint Security konfiguriert wurden, sind nicht mit der aktualisierten Version der Anwendung kompatibel. Wenn Sie zum Verwalten der Anwendung 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).

Konvertierte Richtlinien und Aufgaben erhalten den Namen „*<Name der ursprünglichen Richtlinie oder Aufgabe> (konvertiert)*".

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.

Sie können Richtlinien und Aufgaben nicht in der Kaspersky Security Center Web Console konvertieren.

Wenn Sie zur Verwaltung der Anwendung die Web Console verwenden, müssen Sie in Kaspersky Security Center neue Richtlinien und Aufgaben für die Anwendung erstellen. Sie können einige Einstellungswerte von Richtlinien und Aufgaben aus einer vorherigen Version einer Richtlinie oder Aufgabe in eine neue migrieren, indem Sie Einstellungen exportieren und importieren.

Besonderheiten von Verwaltungs-Plug-ins

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

- Bei der Installation eines neuen Builds des MMC-Plug-ins zur Verwaltung mit der gleichen Versionsnummer wie die Anwendung muss das bereits installierte MMC-Plug-in der gleichen Version gelöscht werden, bevor das neue Plug-in dieser Version installiert werden kann.

Programmeinstellungen nach dem Upgrade

Wenn Sie die Kaspersky Security Center Verwaltungskonsole zur Verwaltung des Programms verwenden, können Sie *Richtlinien konvertieren*, damit die neue Version die Werte der Richtlinieneinstellungen verwendet, die für die vorherige Version des Programms festgelegt wurden (weitere Informationen finden Sie in der Hilfe zu Kaspersky Security Center).

In der Kaspersky Security Center Web Console können keine Richtlinien konvertiert werden.

Nach der Aktualisierung der Anwendung über die Befehlszeile besitzen die meisten Einstellungen jene Werte, die sie bereits in der vorherigen Version der Anwendung besaßen. Sie können die Anwendungseinstellungen auch übertragen, indem Sie die Einstellungen zunächst in eine Datei exportieren und sie anschließend aus der Datei importieren.

Für Einstellungen, die in der früheren Anwendungspersion nicht vorhanden waren, werden die Standardwerte angewendet. Einige Einstellungen verfügen über spezielle Werte.

Abfangen von Systemereignissen

Wenn in der vorherigen Anwendungsversion der Mechanismus zum Abfangen von Systemereignissen basierend auf dem aktualisierbaren Kernel-Modul ausgewählt war, beginnt die Anwendung nach dem Update die fanotify-Technologie zum Abfangen von Systemereignissen zu verwenden. Nach einem anschließenden Update der Datenbanken und Programm-Module sowie einem automatischen Neustart verwendet die Anwendung wieder das aktualisierbare Kernel-Modul.

Einstellungen für „Kaspersky Security Network“

Nach der Konvertierung einer Richtlinie im MMC-Plug-in hängen in den Richtlinieneigenschaften die Einstellungen für die Verwendung von Kaspersky Security Network davon ab, ob Sie im Assistenten zur Richtlinien- und Aufgaben-Konvertierung die Bedingungen der Erklärung zu Kaspersky Security Network akzeptiert oder abgelehnt haben:

- Wenn Sie die Bedingungen der Richtlinie akzeptiert haben, ist die Option **Erweiterter KSN-Modus** ausgewählt.
- Wenn Sie die Bedingungen der Erklärung abgelehnt haben, ist die Option **KSN nicht verwenden** ausgewählt.

Nach dem Update des Programms über die Befehlszeile wird die Einstellung `UseKSN` wie folgt geändert:

- Wenn Sie während des Upgrades `KESL_USE_KSN=No` festlegen, `UseKSN=No`.
- Wenn Sie während des Upgrades `KESL_USE_KSN=Yes` festlegen, `UseKSN=Extended`.
- Für die verbleibenden Fälle ändert sich der Wert des Parameters `UseKSN` nach dem Update nicht.

Einstellungen für die Verwendung des Cloud-Modus

Nach der Konvertierung einer Richtlinie im MMC-Plug-in kann sich die Einstellung für die Verwendung des Cloud-Modus ändern, je nachdem, ob Sie die Bedingungen der KSN-Erklärung im Richtlinien- und Aufgaben-Konvertierungsassistenten akzeptiert oder abgelehnt haben:

- Wenn Sie die Bedingungen der Erklärung akzeptiert haben, wird das Kontrollkästchen **Cloud-Modus aktivieren** aktiviert.
- Wenn Sie die Bedingungen der Erklärung abgelehnt haben, wird das Kontrollkästchen **Cloud-Modus aktivieren** nicht aktiviert.

Nach dem Aktualisieren der Anwendung 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 `UseKSN=Basic/Extended` eingestellt wurde und vor dem Update `CloudMode=Yes` eingestellt war.

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

- Wählen Sie in der Verwaltungskonsole oder in der Web Console die Option **Erweiterter KSN-Modus** aus und aktivieren Sie das Kontrollkästchen **Cloud-Modus aktivieren**.
- Legen Sie in der Befehlszeile die folgenden Einstellungen fest:

```
UseKSN=<Basic|Extended>
CloudMode=Yes
```

Parameter für die Integration mit Kaspersky Managed Detection and Response

Wenn die MDR-Komponente aktiviert war, hängt der Status der MDR-Komponente nach der Konvertierung der Richtlinie im MMC-Plug-in davon ab, ob Sie die Bedingungen der Erklärung zu Kaspersky Security Network im Assistenten zum Konvertieren von Richtlinien und Aufgaben akzeptiert oder abgelehnt haben:

- Wenn Sie die Bedingungen der Erklärung akzeptiert haben, bleibt die MDR-Komponente aktiviert (das Kontrollkästchen **Managed Detection and Response aktivieren** ist aktiviert).
- Wenn Sie die Bedingungen der Erklärung abgelehnt haben, wird das Kontrollkästchen **Managed Detection and Response aktivieren** deaktiviert.

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

- `UseMDR=No`, wenn nach dem Update der Parameter `UseKSN=No` eingestellt ist.
- `UseMDR=Yes`, wenn nach dem Update `UseKSN=Basic/Extended` eingestellt wurde und vor dem Update `UseMDR=Yes` eingestellt war.

Wenn Sie die Funktionen von Kaspersky Managed Detection and Response verwenden möchten, müssen Sie die Verwendung von Kaspersky Security Network im erweiterten Modus aktivieren.

Einstellungen für die Integration in Endpoint Detection and Response Expert

Die neue Version des Programms bietet einen Integrationsmodus für Kaspersky Endpoint Detection and Response Expert (cloud).

Die Integration von Kaspersky Endpoint Security für Linux in Kaspersky Endpoint Detection and Response Expert (cloud) ist vorübergehend nicht verfügbar. Diese Funktionalität wird planmäßig bis Ende 2026 unterstützt. Bitte beachten Sie unsere Versionshinweise. Dort finden Sie aktuelle Informationen über Programm-Upgrades und neue Funktionen.

Nach der Konvertierung der Richtlinie im MMC-Plug-in wird die Integration in Endpoint Detection and Response Expert (cloud) deaktiviert (das Kontrollkästchen **Endpoint Detection and Response Expert (cloud) aktivieren** wird deaktiviert). Das Programm verwendet die Integration in Endpoint Detection and Response Expert (on-premise).

Nach dem Update des Programms über die Befehlszeile wird `EDR_EXPERT_CLOUD_MODE` auf den folgenden Wert festgelegt: `EDR_EXPERT_CLOUD_MODE=No` (Standardwert).

Einstellungen für Benutzerberechtigungen

Die neue Version des Programms unterstützt Kennwortschutz.

Nach der Konvertierung der Richtlinie im MMC-Plug-in ist der Kennwortschutz deaktiviert.

Nach dem Upgrade des Programms über die Befehlszeile bleiben die Benutzerberechtigungen gemäß den Benutzerrollen (*kesladmin*, *kesluser*, *keslaudit*, *nokesl*) erhalten, die in der vorherigen Version des Programms konfiguriert wurden.

Anwendung deinstallieren

Gehen Sie folgendermaßen vor, um Kaspersky Endpoint Security zu deinstallieren.

Besonderheiten bei der Deinstallation von Kaspersky Endpoint Security für Linux

- Während die Anwendung gelöscht wird, werden alle Aufgaben von Kaspersky Endpoint Security auf dem Gerät beendet.
- Nach der Deinstallation des Programms werden alle vom Programm gespeicherten Informationen gelöscht, einschließlich aller installierten Programmzertifikate. Die Lizenzdatenbank bleibt erhalten und Sie können sie für eine erneute Installation der App verwenden. Die eindeutige Computer-ID (SensorID) wird ebenfalls gespeichert.
- Wenn die App auf einem systemd-System installiert wurde, werden die systemd-Einstellungen nach der Deinstallation der App auf ihren ursprünglichen Zustand zurückgesetzt.

1 Deinstallation der Anwendung und der grafischen Oberfläche.

Deinstallieren Sie die Programmpakete und die Pakete der grafischen Benutzeroberfläche von den geschützten Geräten.

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

Sie können die Anwendung und die grafische Oberfläche der Anwendung auf folgende Arten löschen:

Remote mittels Kaspersky Security Center

Lokal über die Befehlszeile

Für die Deinstallation sind Root-Rechte erforderlich.

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

Anwendungspaket und Paket der grafischen Benutzeroberfläche deinstallieren

Deinstallieren Sie das Programm und die grafische Benutzeroberfläche, die aus RPM-Paketen installiert wurden

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

Deinstallieren Sie das Programm und die grafische Benutzeroberfläche, die aus DEB-Paketen installiert wurden

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

Programmpaket entfernen, das ohne grafische Benutzeroberfläche verwendet wurde

```
Entfernen Sie das aus einem RPM-Paket installierte Programm.
```

```
rpm -e kesl
```

```
Entfernen Sie das aus einem DEB-Paket installierte Programm.
```

```
apt-get purge kesl
```

Paket der grafischen Oberfläche deinstallieren

```
Grafische Benutzeroberfläche des aus einem RPM-Paket installierten Programms deinstallieren
```

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

```
Deinstallieren Sie die grafische Benutzeroberfläche des aus einem DEB-Paket installierten Programms
```

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

Die Deinstallation erfolgt im Hintergrund.

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:

Remote mittels Kaspersky Security Center

Lokal über die Befehlszeile

Für die Deinstallation sind Root-Rechte erforderlich.

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

```
Deinstallieren Sie den auf einem 32-Bit-Betriebssystem aus einem RPM-Paket installierten Administrationsagenten
```

```
rpm -e klnagent
```

```
Deinstallieren Sie den auf einem 64-Bit-Betriebssystem aus einem RPM-Paket installierten Administrationsagenten
```

```
rpm -e klnagent64
```

```
Deinstallieren Sie den auf einem 32-Bit-Betriebssystem aus einem DEB-Paket installierten Administrationsagenten
```

```
apt-get purge klnagent
```

```
Deinstallieren Sie den auf einem 64-Bit-Betriebssystem aus einem DEB-Paket installierten Administrationsagenten
```

```
apt-get purge klnagent64
```

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 Administrations-Web-Plug-in oder das MMC-Plug-in von Kaspersky Endpoint Security deinstallieren, je nachdem, welche Konsole Sie zur Verwaltung von Kaspersky Security Center verwendet haben.

So entfernen Sie das MMC-Verwaltungs-Plug-in für Kaspersky Endpoint Security

1. Schließen Sie die Kaspersky Security Center-Verwaltungskonsole.
2. Öffnen Sie auf dem Gerät, auf dem die Kaspersky Security Center Verwaltungskonsole installiert ist, den Windows-Registrierungseditor und wechseln Sie zu:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins
   ```

   Dieser Schlüssel enthält Daten zu allen in der Verwaltungskonsole installierten Verwaltungs-Plug-ins. Der Name der verwalteten Anwendung steht im Parameter **DisplayName**.
3. Wählen Sie den Abschnitt aus, der dem Plug-in für die erforderliche Version der Anwendung Kaspersky Endpoint Security entspricht.
4. Öffnen Sie den Parameter **UninstallString** und kopieren Sie seinen Wert.
5. Öffnen Sie die Befehlszeile mit Administratorrechten, fügen Sie den kopierten Wert ein und drücken Sie die **`Eingabetaste`**.

So entfernen Sie das Web-Verwaltungs-Plug-in für Kaspersky Endpoint Security

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. Aktivieren Sie das Kontrollkästchen **Kaspersky Endpoint Security <version number> für Linux**.
3. Klicken Sie auf die Schaltfläche **Löschen**.

   Bestätigen Sie die Deinstallation des Web-Plug-ins.

Verwenden der App

Standardmäßig wird Kaspersky Endpoint Security automatisch gestartet, wenn das Betriebssystem hochfährt (innerhalb der Standardausführungsebene für jedes Betriebssystem).

Wenn das Programm mit der Standardkonfiguration gestartet wird, werden die folgenden Komponenten 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.

Beim Start der App werden auf dem Gerät automatisch Dienstaufgaben gestartet, um die Ausführung zusätzlicher App-Funktionen sicherzustellen: der Funktion zur App-Aktivierung und der Backup-Funktion.

Standardmäßig führt die Anwendung auch Benutzeraufgaben aus, die in der Befehlszeile konfiguriert sind und die gemäß Startmodus nach dem Start der Anwendung ausgeführt werden sollen (Startmodus `PS`).

Wenn Sie die App beenden, werden alle momentan auf dem Gerät laufenden Aufgaben unterbrochen. Unterbrochene Benutzeraufgaben im PS-Ausführungsmodus werden nicht an der Stelle fortgesetzt, an der sie unterbrochen wurden. Beim nächsten Start des Programms wird eine solche Aufgabe von Anfang an ausgeführt und nicht an der Stelle fortgesetzt, an der sie unterbrochen wurde. Weitere Informationen zu Aufgabentypen finden Sie im Abschnitt Lokale Aufgaben von Kaspersky Endpoint Security.

Der Anwendungsstatus von Kaspersky Endpoint Security wird vom Dienst "Watchdog" überwacht. Der Dienst Watchdog wird beim Start der Anwendung automatisch gestartet. Sollte die Anwendung abstürzen, wird eine Dump-Datei erzeugt und die Anwendung wird automatisch neu gestartet.

So starten oder stoppen Sie die App mithilfe der Web Console

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 Anwendung 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 **Programme**.

4. Aktivieren Sie das Kontrollkästchen neben Kaspersky Endpoint Security.

5. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie die Anwendung starten möchten, klicken Sie auf die Schaltfläche **Starten**.
   - Wenn Sie die Anwendung beenden möchten, klicken Sie auf die Schaltfläche **Beenden**.

Sie können den Status der Anwendungsausführung mithilfe des Widgets **Schutzstatus** im Fenster **Überwachung und Berichterstattung / Dashboard "Überwachung"** überwachen.

So starten oder stoppen Sie die App mithilfe der Verwaltungskonsole

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. Wählen Sie im Kontextmenü des Geräts den Punkt **Eigenschaften** aus.
4. Wählen Sie im Fenster **Eigenschaften: <Name der Anwendung>** den Abschnitt **Anwendungen**.

   Im rechten Teil des Fensters wird eine Liste der auf dem Gerät installierten Kaspersky-Anwendungen angezeigt.
5. Wählen Sie die Anwendung "Kaspersky Endpoint Security" aus.
6. Führen Sie eine der folgenden Aktionen aus:

    – App starten.

    – App stoppen.

   Sie können die App auch über das Kontextmenü verwalten.

So starten oder stoppen Sie die App über die Befehlszeile

Um die Anwendung 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.

Betriebssystem mit systemd

App starten

```
systemctl start kesl
```

App stoppen

```
systemctl stop kesl
```

App neu starten

```
systemctl restart kesl
```

Aktuellen Status der App anzeigen

```
systemctl status kesl
```

Betriebssystem mit init

App starten

```
service kesl start
```

App stoppen

```
service kesl stop
```

App neu starten

```
service kesl restart
```

Aktuellen Status der App anzeigen

```
service kesl status
```

Lizenzverwaltung

Eine *Lizenz* ist ein zeitlich begrenztes Recht zur Nutzung von Kaspersky Endpoint Security, das gemäß dem Endbenutzer-Lizenzvertrag gewährt wird. Der Umfang der verfügbaren Funktionen und die Nutzungsdauer der Anwendung hängen von der Lizenz ab, mit der die Anwendung verwendet wird.

Lizenztypen

Kostenlos

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

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

  Sie können das Programm nur ein Mal mit der Testlizenz aktivieren. Nachdem das Programm mit einer kommerziellen Lizenz aktiviert wurde, kann es nicht mehr mit einer Demolizenz aktiviert werden.

- Die *Demolizenz für Kaspersky Security Center Cloud Console* ist eine Lizenz, die zum Testen der Cloud Console vorgesehen ist. Mit dieser Lizenz können Sie 30 Tage lang 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 Anwendung Kaspersky Endpoint Security mit einer eigenen Testlizenz zu aktivieren, sobald die Testlizenz für der Cloud Console abläuft.

  Der Test-Arbeitsbereich wird nach Ablauf des 30-tägigen Zeitraums automatisch mit seinem gesamten Inhalt gelöscht.

Kostenpflichtig

- *Kommerziell* – kostenpflichtige Lizenz, die beim Erwerb der App zur Verfügung gestellt wird

  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 Gültigkeitsdauer der Lizenz können Sie die Anwendung nicht mehr verwenden und müssen sie von Ihrem Gerät entfernen.

- Ein *Abonnement* ist eine Bestellung für das Programm mit bestimmten Parametern (Ablaufdatum des Abonnements, Anzahl der geschützten Geräte). Sie können ein Abonnement bei einem Dienstanbieter in Ihrer Region erwerben.

  Es gibt beschränkte (z. B. auf ein Jahr) und unbefristete (ohne Ablaufdatum) Abos. Nach Ablauf eines befristeten Abonnements wird möglicherweise eine Nachfrist zur Abo-Verlängerung gewährt, während der die Programmfunktionalität erhalten bleibt. Ob es eine Nachfrist gibt und wie lang diese ist, wird vom Dienstanbieter bestimmt.

  Sie können Ihr Abonnement, einschließlich dessen Kündigung, auf der Website des Dienstanbieters verwalten.

So funktioniert die Lizenzierung

1. **Sie erhalten einen Aktivierungscode**

   Nachdem Sie eine Kaspersky-Lösung auf der offiziellen Kaspersky-Website oder bei einem unserer Partner erworben haben, erhalten Sie eine Nachricht an die E-Mail-Adresse, die Sie beim Kauf angegeben haben. Diese Nachricht enthält einen Aktivierungscode und Informationen darüber, wie Sie eine Schlüsseldatei erhalten. Sie benötigen möglicherweise eine Schlüsseldatei, wenn Ihr Unternehmen die Online-Aktivierung des Programms mithilfe eines Codes nicht unterstützt.

   Wenn Sie ein Abonnement für Kaspersky Endpoint Security erworben haben, stellt Ihnen der Dienstanbieter nur einen Aktivierungscode zur Verfügung.

2. **Programm aktivieren**

   Anschließend müssen Sie *das Programm aktivieren*, d. h. eine Programmlizenz gültig machen. Dazu müssen Sie dem Programm mithilfe Ihres Aktivierungscodes oder Ihrer Schlüsseldatei einen Lizenzschlüssel hinzufügen.

   Es sind folgende Aktivierungsmethoden vorgesehen:

   - Per Fernzugriff mithilfe von Kaspersky Security Center
   - Über die Befehlszeile
   - Über die grafische Benutzeroberfläche

   Standard-Modus

Um das Programm im Standard-Modus zu verwenden, können Sie Lizenzen, die unterschiedliche Funktionsumfänge abdecken, verwenden. Wenn einige Komponenten nicht durch Ihre Lizenz abgedeckt sind, benötigen Sie möglicherweise einen anderen Lizenzschlüssel:

- Lizenzschlüssel für das Add-on Kaspersky Endpoint Detection and Response Optimum (im Folgenden auch als *EDR Optimum-Schlüssel* bezeichnet) zum Aktivieren der Kaspersky EDR Optimum-Komponente
- Lizenzschlüssel für das Add-on Kaspersky Unified Monitoring and Analysis Platform (im Folgenden auch als *KUMA-Schlüssel* bezeichnet) zum Aktivieren der Integration mit der Funktionalität von Kaspersky Unified Monitoring and Analysis Platform
- Lizenzschlüssel für das Add-on Kaspersky Managed Detection and Response Optimum/Expert (im Folgenden auch als *MDR-Schlüssel* bezeichnet) zum Aktivieren der Kaspersky MDR-Komponente
- Lizenzschlüssel für das Add-on Kaspersky Endpoint Detection and Response Expert (on-premises) (im Folgenden auch als *EDR Expert (on-premises)-Schlüssel* bezeichnet) zum Aktivieren der EDR Expert (on-premises)-Komponente
- Lizenzschlüssel für das Add-on Kaspersky Endpoint Detection and Response Expert (cloud) (im Folgenden auch als *EDR Expert (cloud)-Schlüssel* bezeichnet) zum Aktivieren der EDR Expert (cloud)-Komponente
- Lizenzschlüssel für das Add-on Kaspersky Workload Security Module (im Folgenden auch als *KWSM-Schlüssel* bezeichnet) zum Aktivieren der Komponenten Überwachung der Systemintegrität und Untersuchung von Containern

Wenn diese Komponenten nicht durch Ihre Lizenz abgedeckt sind, können Sie sie erst aktivieren, nachdem Sie das Programm Kaspersky Endpoint Security selbst aktiviert haben.

EDR Agent-Modus

Wenn Sie das Programm Kaspersky Endpoint Security im EDR-Agent-Modus verwenden, benötigen Sie zur Aktivierung einen Lizenzschlüssel für EDR Expert (on-premise).

Light Agent-Modus

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus verwenden, müssen Sie dem Programm keinen Schlüssel hinzufügen. Sie aktivieren Kaspersky Security for Virtualization Light Agent auf der Seite des Schutzservers.

Die Komponente Endpoint Detection and Response Optimum und die Komponenten für die Integration mit Kaspersky-Lösungen werden ebenfalls auf der Seite des Schutzservers aktiviert.

Fehlerbehebung bei Problemen mit der Programmaktivierung

3. **Lizenz oder Abonnement verlängern**

Wir empfehlen Ihnen, Ihre Lizenz bzw. Ihr Abonnement im Blick zu behalten, um sie rechtzeitig zu verlängern. 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.

Zur rechtzeitigen Verlängerung der Lizenz können Sie einen Reserveschlüssel verwenden. Sie können Ihr Abonnement manuell oder automatisch auf der Webseite Ihres Dienstanbieters verlängern. Ein unbefristetes Abonnement wird automatisch verlängert, wenn die Gebühren des Händlers rechtzeitig bezahlt wurden.

Besonderheiten beim Hinzufügen von Schlüsseln

- Ein Lizenzschlüssel für eine Demolizenz oder ein Abonnementschlüssel kann nicht als Reserveschlüssel hinzugefügt werden.
- Das Ablaufdatum des Reserveschlüssels muss nach dem Ablaufdatum des aktiven Schlüssels liegen.

- Wenn dem Programm sowohl ein aktiver Schlüssel als auch ein Reserveschlüssel hinzugefügt wurden und Sie einen neuen aktiven Schlüssel hinzufügen, ersetzt der neue Schlüssel den zuvor hinzugefügten aktiven Schlüssel; wenn Sie einen neuen Reserveschlüssel hinzufügen, ersetzt dieser den zuvor hinzugefügten Reserveschlüssel.

- Wenn dem Programm ein aktiver Schlüssel sowie Schlüssel zum Aktivieren der Komponente Endpoint Detection and Response Optimum und der Komponenten für die Integration mit Kaspersky-Lösungen hinzugefügt wurden und Sie einen Reserveschlüssel für eine Lizenz hinzugefügt haben, die ebenfalls die Komponente Endpoint Detection and Response Optimum und die Komponenten für die Integration abdeckt, wird der Reserveschlüssel nach Ablauf des aktiven Schlüssels aktiv und gibt die anderen aktiven Schlüssel frei. Anschließend können Sie diese Schlüssel verwenden, um die Komponente Endpoint Detection and Response Optimum und die Komponenten für die Integration auf einem anderen Gerät zu aktivieren.

4. **Informationen über hinzugefügte Lizenzschlüssel anzeigen**

   Sie können Informationen über Lizenzschlüssel anzeigen, die dem Programm hinzugefügt wurden, und zwar remote mithilfe von Kaspersky Security Center oder lokal auf einem geschützten Gerät mithilfe der Befehlszeile oder der grafischen Benutzeroberfläche.

Nützliche Artikel

Endbenutzer-Lizenzvertrag

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

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

Sie können den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie, in der die Verarbeitung und Bereitstellung von Daten beschrieben wird, lesen:

- Vor der Installation des Programms in der Datei license.<Sprachkennung>. Diese Datei gehört zum Lieferumfang des der Anwendung.
- Während der Installation der Anwendung Kaspersky Endpoint Security.

  Indem Sie beim Erstellen des Installationspakets für das Programm (bei Installation mithilfe von Kaspersky Security Center) oder während der Erstkonfiguration des Programms (bei Installation über die Befehlszeile) Ihre Zustimmung zu den Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie bestätigen, akzeptieren Sie die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie. 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 des Programms befinden sich die Dateien mit den Texten des Endbenutzer-Lizenzvertrags des Kaspersky-Programms und der Datenschutzrichtlinie auf dem geschützten Gerät im Verzeichnis /opt/kaspersky/kesl/doc/license.<Sprach-ID>.

Aktivierungscode

Ein *Aktivierungscode* ist eine einmalige Sequenz aus zwanzig lateinischen Buchstaben und Ziffern.

Um das Programm mithilfe eines Aktivierungscodes zu aktivieren, ist ein Internetzugang für die Verbindung mit den Aktivierungsservern von Kaspersky 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.

Schlüsseldatei

Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung key, die Sie von Kaspersky erhalten. Um das Programm mithilfe einer Schlüsseldatei zu aktivieren, müssen Sie keine Verbindung zu den Kaspersky-Aktivierungsservern herstellen.

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.
- Fordern Sie auf der Kaspersky-Website mithilfe Ihres vorhandenen Aktivierungscodes eine Schlüsseldatei an.

Lizenzschlüssel

Ein *Lizenzschlüssel* ist eine Bitsequenz, mit der Sie das Programm in Übereinstimmung mit den Bedingungen des Endbenutzer-Lizenzvertrags aktivieren und anschließend verwenden können. Der Lizenzschlüssel wird von Kaspersky erstellt.

Der Schlüssel, mit dem das Programm derzeit aktiviert ist, wird zum *aktiven Lizenzschlüssel*. Als aktiven Schlüssel können Sie einen Demolizenzschlüssel, einen kommerziellen Lizenzschlüssel (kommerziellen Schlüssel) oder einen Abonnementschlüssel hinzufügen.

Reserveschlüssel

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 erst hinzugefügt werden, nachdem ein aktiver Schlüssel hinzugefügt wurde.

Der Lizenzschlüssel einer Testlizenz kann nur als aktiver Schlüssel hinzugefügt werden. Ein Lizenzschlüssel für eine Demolizenz kann nicht als Reserve-Lizenzschlüssel hinzugefügt werden.

So wechseln Sie zu einer anderen Kaspersky-Lösung

Wenn die App im Light Agent-Modus verwendet wird, werden die Lizenzschlüssel in der Lösung Kaspersky Security for Virtualization Light Agent verwaltet.

Führen Sie die folgenden Schritte aus, wenn in Ihrem Unternehmen eine Kaspersky-Lösung bereitgestellt ist, Kaspersky Endpoint Security im Standard-Modus oder im EDR Agent-Modus verwendet wird und Sie zu einer anderen Kaspersky-Lösung wechseln müssen.

1. **Neue Lizenz vorbereiten**

   Erwerben Sie eine andere Kaspersky-Lösung auf der Kaspersky-Website oder bei unseren Partnern. Sie erhalten eine E-Mail an die E-Mail-Adresse, die Sie beim Kauf angegeben haben. Diese Nachricht enthält einen Aktivierungscode und Informationen darüber, wie Sie eine Schlüsseldatei erhalten.

   Wenn Sie das Programm Kaspersky Endpoint Security zuvor mithilfe eines Aktivierungscodes aktiviert haben, müssen Sie diesmal ebenfalls einen Aktivierungscode verwenden. Wenn Sie das Programm zuvor mithilfe einer Schlüsseldatei aktiviert haben, müssen Sie eine Schlüsseldatei verwenden.

2. **Lizenz ersetzen**

   Sie können eine Lizenz auf folgende Weise ersetzen:

   - Per Fernzugriff über Kaspersky Security Center. Fügen Sie den Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzu und verteilen Sie ihn auf geschützte Geräte.
   - Über die Befehlszeile mit folgendem Befehl: `kesl-control [-L] --add-active-key <path to key file / activation code>`.
   - Löschen Sie in der grafischen Benutzeroberfläche den Schlüssel, der derzeit für das Programm verwendet wird, und fügen Sie den neuen Schlüssel hinzu.

3. **Sicherstellen, dass die Lizenz erfolgreich ersetzt wurde**

   Dazu zeigen Sie die Details des Lizenzschlüssels an, der auf Ihren geschützten Geräten verwendet wird.

Nützliche Artikel

Aktivierungscode

Ein *Aktivierungscode* ist eine einmalige Sequenz aus zwanzig lateinischen Buchstaben und Ziffern.

Um das Programm mithilfe eines Aktivierungscodes zu aktivieren, ist ein Internetzugang für die Verbindung mit den Aktivierungsservern von Kaspersky 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.

Schlüsseldatei

Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung key, die Sie von Kaspersky erhalten. Um das Programm mithilfe einer Schlüsseldatei zu aktivieren, müssen Sie keine Verbindung zu den Kaspersky-Aktivierungsservern herstellen.

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.
- Fordern Sie auf der Kaspersky-Website mithilfe Ihres vorhandenen Aktivierungscodes eine Schlüsseldatei an.

Lizenzschlüssel verwalten

Wenn die App im Light Agent-Modus verwendet wird, werden die Lizenzschlüssel in der Lösung Kaspersky Security for Virtualization Light Agent verwaltet. Befehle zur Verwaltung der Lizenzschlüssel werden mit einem Fehler beendet.

Schlüsselverwaltung mithilfe von Kaspersky Security Center

In Kaspersky Security Center können Sie Schlüssel auf folgende Arten zu verwalteten Geräten hinzufügen:

- Mithilfe der Aufgabe *Schlüssel hinzufügen*. Mit dieser Methode können Schlüssel zur App auf einem einzelnen Gerät oder auf allen Geräten hinzugefügt werden, die einer Administrationsgruppe angehören. Beim Erstellen einer Aufgabe wird jener Schlüssel verwendet, der zum Schlüsselspeicher von Kaspersky Security Center hinzugefügt wurde. Sie können dem Schlüsselspeicher im Voraus oder beim Erstellen der Aufgabe „Schlüssel hinzufügen“ einen Lizenzschlüssel hinzufügen.
- Durch Verteilen eines auf dem Kaspersky Security Center Administrationsserver gespeicherten Schlüssels an die Geräte. Mit dieser Methode können Schlüssel automatisch zu verwalteten Geräten hinzugefügt werden, die bereits mit Kaspersky Security Center verbunden sind, sowie zu neuen verwalteten Geräten. Um diese Methode nutzen zu können, müssen Sie den Schlüssel zunächst dem Schlüsselspeicher von Kaspersky Security Center hinzufügen.

  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**.

So fügen Sie mithilfe der Web Console einen 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 **Schlüsseldatei auswählen** und wählen Sie im nächsten 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 mithilfe einer Aufgabe „Schlüssel hinzufügen“ einen Schlüssel hinzu

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** den 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 aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.

   Das Fenster **Lizenz auswählen** 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 der benötigte Schlüssel nicht im Schlüsselspeicher vorhanden ist, klicken Sie auf den Link **neuen Lizenzschlüssel 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 **Schlüsseldatei auswählen** und wählen Sie im nächsten 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. Auf der Registerkarte **Programmeinstellungen** können Sie das Kontrollkästchen **Als Reserveschlüssel verwenden** aktivieren. Ein als Reserveschlüssel hinzugefügter Schlüssel wird nach Ablauf des aktuellen Schlüssels aktiv.
9. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.
10. Aktivieren Sie das Kontrollkästchen neben der Aufgabe. Klicken Sie auf **Starten**.

So fügen Sie der App mithilfe der Web Console einen Schlüssel hinzu, indem Sie den Schlüssel an Geräte verteilen

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 Anwendung, 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.

> Ein neuer Lizenzschlüssel wird dem Gerät nur hinzugefügt, wenn die Anwendung auf diesem Gerät noch nicht aktiviert ist oder die Lizenz in weniger als 14 Tagen abläuft.

Schlüsselverwaltung über die Befehlszeile

Um die Lizenzschlüssel auf einem Gerät zu verwalten, können Sie die Befehle zur Verwaltung von Lizenzschlüsseln verwenden.

So fügen Sie der App einen Schlüssel hinzu

Mit diesen Befehlen können Sie Schlüssel zur Aktivierung des Programms sowie Schlüssel zur Aktivierung von Komponenten hinzufügen, die nicht durch Ihre Lizenz abgedeckt sind. Der Schlüsseltyp muss nicht im Befehl angeben werden.

Aktiven Lizenzschlüssel zur App hinzufügen

```
kesl-control [-L] --add-active-key <path to key file / activation code>
```

Wobei gilt:

- `path to key file` ist der Pfad zur Schlüsseldatei. Wenn sich die Schlüsseldatei im aktuellen Verzeichnis befindet, ist die Angabe des Dateinamens ausreichend.
- `activation code` ist der Aktivierungscode.

Reserve-Lizenzschlüssel zur App hinzufügen

```
kesl-control [-L] --add-reserve-key <path to key file / activation code>
```

Wenn der Anwendung auf dem Gerät noch kein aktiver Schlüssel hinzugefügt wurde, schlägt der Befehl fehl.

So löschen Sie einen Schlüssel

Zum Löschen von Schlüsseln stehen verschiedene Befehle zur Verfügung.

Aktiven Schlüssel löschen

```
kesl-control [-L] --remove-active-key
```

Reserveschlüssel löschen

```
kesl-control [-L] --remove-reserve-key
```

Aktiven Schlüssel für EDR Optimum löschen

```
kesl-control [-L] --remove-active-key --edr-optimum
```

Reserveschlüssel für EDR Optimum löschen

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

Aktiven Schlüssel für KUMA löschen

```
kesl-control [-L] --remove-active-key --kuma
```

Reserveschlüssel für KUMA löschen

```
kesl-control [-L] --remove-reserve-key --kuma
```

Aktiven Schlüssel für MDR löschen

```
kesl-control [-L] --remove-active-key --mdr
```

Reserveschlüssel für MDR löschen

```
kesl-control [-L] --remove-reserve-key --mdr
```

Aktiven Lizenzschlüssel für EDR Expert (on-premise) löschen

```
kesl-control [-L] --remove-active-key --edr-kata
```

Reserve-Lizenzschlüssel für EDR Expert (on-premise) löschen

```
kesl-control [-L] --remove-reserve-key --edr-kata
```

Aktiven Schlüssel für EDR Expert (cloud) löschen

```
kesl-control [-L] --remove-active-key --cxdr
```

Reserveschlüssel für EDR Expert (cloud) löschen

```
kesl-control [-L] --remove-reserve-key --cxdr
```

Aktiven Schlüssel für KWSM löschen

```
kesl-control [-L] --remove-active-key --khcs
```

Reserveschlüssel für KWSM löschen

```
kesl-control [-L] --remove-reserve-key --khcs
```

Schlüsselverwaltung über die grafische Benutzeroberfläche

So fügen Sie einen aktiven Lizenzschlüssel hinzu

1. Öffnen Sie das Hauptfenster der grafischen Benutzeroberfläche des Programms.
2. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie im unteren Teil des Hauptfensters auf den Bereich des Fensters, in dem Informationen zur Lizenz und zum Schlüssel angezeigt werden.
   - Klicken Sie im unteren Teil des Hauptfensters auf die Schaltfläche **Support** und öffnen Sie im nächsten Fenster **Support** und klicken Sie auf den Link im Feld **Lizenzschlüssel** oder auf den Link **Lizenzen** im unteren Teil des Fensters.

   Das Fenster **Lizenzen** 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. Wenn Sie die Anwendung unter einer kommerziellen Lizenz aktivieren möchten:

   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, öffnen Sie das Fenster zur Dateiauswahl anhand des Links **Schlüsseldatei auswählen** und wählen Sie neuen Fenster eine Datei mit key-Erweiterung aus.

      In diesem Fenster werden Informationen über den Schlüssel und die mit ihm verbundene Lizenz angezeigt.

   b. Klicken Sie auf **Aktivieren**.

4. Wenn Sie die Anwendung mit einer Testlizenz aktivieren möchten, klicken Sie im Block **Testschlüssel** auf die Schaltfläche **Aktivieren**. In diesem Fenster werden Informationen über die Demolizenz und den damit verbundenen Schlüssel angezeigt.

So fügen Sie einen Reserve-Lizenzschlüssel hinzu

1. Öffnen Sie das Hauptfenster der grafischen Benutzeroberfläche des Programms.

2. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie im unteren Teil des Hauptfensters auf den Bereich des Fensters, in dem Informationen zur Lizenz und zum Schlüssel angezeigt werden.

   - Klicken Sie im unteren Teil des Hauptfensters auf die Schaltfläche **Support** und öffnen Sie im nächsten Fenster **Support** und klicken Sie auf den Link im Feld **Lizenzschlüssel** oder auf den Link **Lizenzen** im unteren Teil des Fensters.

   Das Fenster **Lizenzen** wird geöffnet. Das Fenster zeigt Informationen über zuvor hinzugefügte Lizenzschlüssel an.

3. Klicken Sie 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, öffnen Sie das Fenster zur Dateiauswahl anhand des Links **Schlüsseldatei auswählen** und wählen Sie neuen Fenster eine Datei mit key-Erweiterung aus.

   In diesem Fenster werden Informationen über den Schlüssel und die mit ihm verbundene Lizenz angezeigt.

4. Klicken Sie auf **Hinzufügen**.

So entfernen Sie einen Lizenzschlüssel

1. Öffnen Sie das Hauptfenster der grafischen Benutzeroberfläche des Programms.
2. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie im unteren Teil des Hauptfensters auf den Bereich des Fensters, in dem Informationen zur Lizenz und zum Schlüssel angezeigt werden.
   - Klicken Sie im unteren Teil des Hauptfensters auf die Schaltfläche **Support** und öffnen Sie im nächsten Fenster **Support** und klicken Sie auf den Link im Feld **Lizenzschlüssel** oder auf den Link **Lizenzen** im unteren Teil des Fensters.

   Das Fenster **Lizenzen** wird geöffnet. Das Fenster zeigt Informationen über zuvor hinzugefügte Lizenzschlüssel an.
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.

Nützliche Artikel

Fehlerbehebung bei Problemen mit der Programmaktivierung

Informationen zu Lizenzschlüsseln anzeigen

Informationen zu Lizenzschlüsseln in Kaspersky Security Center

Sie können Informationen zu den von Kaspersky Endpoint Security verwendeten Lizenzschlüsseln auf folgende Weise anzeigen:

- In den Eigenschaften der Aufgabe *Schlüssel hinzufügen*, mit der Sie das Programm aktivieren, finden Sie Informationen zu dem Schlüssel, den diese Aufgabe zum Programm hinzufügt.
- In den Eigenschaften des auf dem Client-Gerät installierten Kaspersky-Programms finden Sie Informationen zu dem aktiven Schlüssel und dem Reserveschlüssel, die dem Programm auf diesem Gerät hinzugefügt wurden.

  So zeigen Sie Informationen zu Lizenzschlüsseln auf einem Gerät mithilfe der Web Console an

  1. Wählen Sie im Hauptfenster der Web Console **Asset-Management → Assets (Geräte)** aus.

     Die Liste der verwalteten Geräte wird geöffnet.
  2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Um eine verschachtelte Gruppe auszuwählen, klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Hierarchie anzeigen**.

     In der Liste werden nur die verwalteten Geräte der ausgewählten Administrationsgruppe angezeigt.
  3. Klicken Sie auf den Namen eines Geräts.

4. Wechseln Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts zur Registerkarte **Anwendungen**.

5. Klicken Sie in der Liste der auf dem Gerät installierten Anwendungen auf den Namen der Anwendung Kaspersky Endpoint Security.

6. Daraufhin wird das Fenster mit den Programmeigenschaften geöffnet; wechseln Sie in diesem Fenster auf der Registerkarte **Allgemein** zum Abschnitt **Lizenzen**.

   Der Abschnitt enthält Informationen über die der Anwendung hinzugefügten Lizenzschlüssel und über die mit diesen Schlüsseln verknüpften Lizenzen:

   - Der **Lizenzschlüsselstatus** gibt den Typ des Schlüssels an: aktiv oder Reserve.
   - **Name der Anwendung** – Name der mit dem Schlüssel verknüpften Lizenz und Informationen zu dieser Lizenz
   - **Lizenzschlüssel** – Lizenzschlüssel: eindeutige alphanumerische Zeichenfolge
   - **Lizenztyp** – Lizenztyp: Test, kommerziell oder Abonnement
   - **Aktivierungsdatum** – Datum, an dem der Schlüssel hinzugefügt wurde
   - **Ablaufdatum** – Zeitpunkt, an dem Nutzungsdauer der Anwendung abläuft, die mithilfe des Schlüssels aktiviert wurde

So zeigen Sie Informationen zu Lizenzschlüsseln auf einem Gerät mithilfe der Verwaltungskonsole 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 Kaspersky-Anwendungen angezeigt.

5. Wählen Sie Kaspersky Endpoint Security aus und doppelklicken Sie darauf, um das Fenster mit den Programmeigenschaften zu öffnen. Alternativ können Sie die Schaltfläche **Eigenschaften** im unteren Bereich des Fensters verwenden.

6. Wechseln Sie im geöffneten Fenster zum Abschnitt **Lizenzschlüssel**.

   Der Abschnitt 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.
   - **Gültigkeitsdauer der Lizenz**: Anzahl der Tage, an denen Sie das durch Hinzufügen dieses Schlüssels aktivierte Programm verwenden können.

- **Lizenzbeschränkung**: Anzahl der Geräte, auf denen Sie den Schlüssel verwenden können.
- **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 Anwendung, welche durch das Hinzufügen eines aktiven Schlüssels aktiviert wurde.

- Der Bericht über die Verwendung von Lizenzschlüsseln zeigt Informationen zu allen Schlüsseln an, die mithilfe von Kaspersky Security Center hinzugefügt wurden. Sie können den Bericht über die Verwendung von Lizenzschlüsseln über die Web Console (**Überwachung und Berichterstattung → Berichte**) sowie über die Verwaltungskonsole (Registerkarte **Berichte**) anzeigen. Um den Bericht anzuzeigen, müssen Sie in der Liste mit den Berichten die Vorlage "Bericht über die Lizenzschlüsselnutzung" auswählen und mit der Erstellung des Berichts beginnen.
- Der Lizenzschlüsselspeicher von Kaspersky Security Center zeigt Informationen zu allen Schlüsseln an, die zum Kaspersky Security Center Administrationsserver hinzugefügt wurden. Sie können den Schlüsselspeicher sowohl über die Web Console (**Vorgänge → Lizenzen von Kaspersky**) als auch über die Verwaltungskonsole (Ordner **Lizenzen von Kaspersky**) öffnen.

Außerdem können Sie Informationen über die verwendeten Lizenzschlüssel und die damit verknüpften Lizenzen auch über die Ereignisbenachrichtigungen von Kaspersky Security Center erhalten. Die Anwendung sendet an den Kaspersky Security Center Administrationsserver Informationen über den Ablauf der Lizenz und die Verletzung von Lizenzbeschränkungen.

Informationen zu Lizenzschlüsseln auf dem geschützten Gerät

So zeigen Sie Informationen zu Lizenzschlüsseln über die Befehlszeile an

```
Anzeigen von Informationen zu Lizenzschlüsseln und Lizenzen auf einem Gerät

kesl-control -L --query [--json]
```

Dabei bedeutet `--json` die Ausgabe von Daten im JSON-Format. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen in die Konsole ausgegeben.

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

- Informationen zum aktiven Lizenzschlüssel:
  - Ablaufdatum und -uhrzeit der Lizenz.
  - Die Anzahl der Tage bis zum Ablauf der Gültigkeitsdauer der Lizenz.
  - Informationen über die Einschränkung der Schutzfunktionalität (diese Zeile wird nur für den Schlüssel angezeigt, mit dem das Programm Kaspersky Endpoint Security aktiviert ist).
  - Informationen zu Einschränkungen beim Update der Datenbanken des Programms.
  - Informationen zum Status des Lizenzschlüssels.
  - Der mit dem Schlüssel verknüpfte Lizenztyp.
  - Beschränkung des Lizenzschlüssels (Anzahl der Lizenzierungseinheiten).

- Der Name der Anwendung, die der Schlüssel aktivieren soll.
- Aktiver Lizenzschlüssel (eindeutige alphanumerische Zeichenfolge).
- Datum der Aktivierung.

- Informationen zum Reserve-Lizenzschlüssel. Wird angezeigt, wenn das Programm im Standard-Modus oder im EDR Agent-Modus verwendet wird und ein Reserveschlüssel hinzugefügt wurde. Wenn das Programm im Light Agent-Modus verwendet wird, werden Informationen zum Reserveschlüssel nicht angezeigt.
  - Ablaufdatum und -uhrzeit der Lizenz.
  - Informationen über die Einschränkung der Schutzfunktionalität (diese Zeile wird nur für einen Schlüssel angezeigt, mit dem das Programm Kaspersky Endpoint Security aktiviert werden kann).
  - Informationen zu Einschränkungen beim Update der Datenbanken des Programms.
  - Informationen zum Status des Lizenzschlüssels.
  - Der mit dem Schlüssel verknüpfte Lizenztyp.
  - Beschränkung des Lizenzschlüssels (Anzahl der Lizenzierungseinheiten).
  - Der Name der Anwendung, die der Schlüssel aktivieren soll.
  - Reserve-Lizenzschlüssel (eindeutige alphanumerische Zeichenfolge).
  - Zeitpunkt des Ablaufs der mit dem aktiven Schlüssel verknüpften Lizenz.

Informationen zur Lizenz, unter der das Programm verwendet wird, können Sie auch beim Anzeigen der Programmdetails erhalten:

```
kesl-control --app-info
```

So zeigen Sie Lizenz- und Schlüsselinformationen in der grafischen Benutzeroberfläche des Programms an

1. Öffnen Sie das Hauptfenster der grafischen Benutzeroberfläche des Programms.
2. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie im unteren Teil des Hauptfensters auf den Bereich des Fensters, in dem Informationen zur Lizenz und zum Schlüssel angezeigt werden.
   - Klicken Sie im unteren Teil des Hauptfensters auf die Schaltfläche **Support** und öffnen Sie im nächsten Fenster **Support** und klicken Sie auf den Link im Feld **Lizenzschlüssel** oder auf den Link **Lizenzen** im unteren Teil des Fensters.

   Das Fenster **Lizenzen** wird geöffnet.

   Das Fenster zeigt Informationen über die der Anwendung hinzugefügten aktiven Schlüssel und Reserveschlüssel an. Klicken Sie auf **Mehr erfahren**, um die vollständigen Informationen zu den Lizenzen und Schlüsseln anzuzeigen.

Im Abschnitt **Aktuelle Lizenzen** werden Informationen zu hinzugefügten aktiven Schlüsseln und zugehörigen Lizenzen angezeigt:

- Typ der Lizenz, Lizenzbeschränkungen und Ablaufdatum der Lizenz.
- **Lizenzschlüssel** – Eindeutige alphanumerische Zeichenfolge.
- **Schlüsselstatus** – Status des Schlüssels oder eine Benachrichtigung über etwaige Probleme mit dem Schlüssel.
- **Aktivierungsdatum** – Datum der Aktivierung der Anwendung durch Hinzufügen dieses Schlüssels.
- **Verbleibend** – Anzahl der Tage bis zum Ablauf der Lizenz und Ablaufdatum der Lizenz im UTC-Format.
- **Name** – Der Name der Anwendung, für deren Aktivierung der Schlüssel vorgesehen ist.
- **Schutz** – Informationen über Einschränkungen der Schutzfunktionen und über die Aktualisierung von App-Datenbanken.

Im Abschnitt **Reserveschlüssel** werden Informationen zu hinzugefügten Reserveschlüsseln und zugehörigen Lizenzen angezeigt:

- Typ des Reserveschlüssels, Lizenzbeschränkungen und Ablaufdatum der mit dem Schlüssel verknüpften Lizenz.
- **Lizenzschlüssel** – Eindeutige alphanumerische Zeichenfolge.
- **Lizenztyp** – Typ der mit dem Sicherungsschlüssel verknüpften Lizenz.
- **Name** – Der Name der Anwendung, für deren Aktivierung der Schlüssel vorgesehen ist.
- **Schutz** – Informationen über Einschränkungen der Schutzfunktionen und über die Aktualisierung von App-Datenbanken.

Wenn Sie Kaspersky Endpoint Security im Standard-Modus oder im EDR Agent-Modus verwenden und das Programm mithilfe von Kaspersky Security Center verwalten, werden standardmäßig Informationen zum Hinzufügen und Entfernen von Lizenzschlüsseln sowie zum Ablauf der Gültigkeitsdauer der Lizenz im Betriebssystemprotokoll aufgezeichnet.

Verwaltungsschnittstellen der App

Zur Verwaltung von Kaspersky Endpoint Security können Sie Folgendes verwenden:

- Kaspersky Security Center
- Befehlszeile
- Grafische Oberfläche der Anwendung

  Über die grafische Benutzeroberfläche von Kaspersky Endpoint Security können Sie nur eine begrenzte Anzahl von Aktionen ausführen.

Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, kann die Anwendung nicht über die Kaspersky Security Center Cloud Console und die grafische Benutzeroberfläche der Anwendung verwaltet werden.

Wenn die Anwendung im EDR Agent-Modus verwendet wird, ist nur ein begrenzter Teil der Programmkomponenten und Aufgaben verfügbar. Sie können bestimmte Schutzkomponenten verwalten, die Anwendung aktivieren und ein Update der Datenbanken durchführen. Weitere Informationen zu den Besonderheiten des EDR-Agent-Modus finden Sie im Artikel Bekannte Probleme und Einschränkungen.

Wählen Sie ein Verwaltungstool entsprechend der IT-Infrastruktur Ihres Unternehmens sowie der Rolle und dem Arbeitsablauf des Administrators aus. Es wird empfohlen, die Anwendung auf Client-Geräten zentral über Kaspersky Security Center zu verwalten.

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 Anwendung anpassen sowie Aufgaben auf den verwalteten Geräten starten und beenden.

Administrationsgruppen von Kaspersky Security Center

Um mithilfe von Kaspersky Security Center das auf den Geräten installierte Kaspersky Endpoint Security zu verwalten, müssen Sie diese Geräte zu *Administrationsgruppen* hinzufügen. 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. Sie können die Geräte nach der Installation des Programms auch manuell in die Administrationsgruppen verschieben (Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security Center).

Verwaltungskonsolen und Verwaltungs-Plug-ins

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 von Kaspersky Endpoint Security (im Folgenden auch „MMC-Plug-in“ genannt) bereitgestellt.

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

- 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-Anwendungen. Sie können in Kaspersky Security Center Web Console über einen Browser auf einem beliebigen Gerät arbeiten.

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

Das Web-Plug-in muss auf dem Gerät installiert werden, auf dem Kaspersky Security Center Web Console installiert ist.

- 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 Oberfläche dieser Cloud-Konsole entspricht der Oberfläche 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.

  Die Verwaltung des Programms mit Kaspersky Security Center Cloud Console ist nicht möglich, wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird.

Kaspersky Endpoint Security ist Teil der Lösung Kaspersky Next Pro View. Weitere Informationen zu verfügbaren Funktionen im Rahmen dieser Lösung finden Sie in der Hilfe zu Kaspersky Next.

Richtlinien und Aufgaben von Kaspersky Security Center

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 Anwendungsausführung 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 Anwendung 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, Anwendungsaktivierung sowie Update der Datenbanken und Module der Anwendung.

  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).

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. Die Richtlinie hat einen der folgenden Status:

Richtlinienstatus

Zustand	Description
Aktiv	Die aktuelle Richtlinie, die auf das Gerät angewendet wird.
Inaktiv	Eine Richtlinie, die derzeit nicht auf das Gerät angewendet wird.
Mobil	Wenn diese Option ausgewählt ist, tritt die Richtlinie in Kraft, wenn das Gerät das Netzwerk der Organisation verlässt.

Für Richtlinien gelten folgende Regeln:

- Sie können mehrere Richtlinien mit unterschiedlichen Einstellungen für ein Programm konfigurieren.
- Pro Programm kann nur eine Richtlinie aktiv sein.
- Eine Richtlinie kann untergeordnete Richtlinien haben.

Sperren von Einstellungen

Jede Richtlinieneinstellung hat das Attribut „Vorhängeschloss“. Der Status dieses Attributs bestimmt, ob die Einstellung auf die verwalteten Geräte in der Administrationsgruppe übertragen wird.

- Wenn das „Vorhängeschloss“ geschlossen ist (🔒), bedeutet dies, dass die Einstellung auf die Geräte angewendet wird, auf die die Richtlinie angewendet wird. Der Benutzer kann solche Einstellungen in der Benutzeroberfläche des verwalteten Programms nicht ändern. Solche Einstellungen werden *gesperrt* genannt.
- Wenn das „Vorhängeschloss“ geöffnet ist (🔓), bedeutet dies, dass die Einstellung nicht in der Richtlinie angegeben ist. Der Benutzer kann solche Einstellungen in der Benutzeroberfläche des verwalteten Programms ändern. Solche Einstellungen werden *entsperrt* genannt.

Wir empfehlen, die Richtlinieneinstellungen zu sperren, die Sie auf verwaltete Geräte anwenden möchten. Nicht gesperrte Richtlinieneinstellungen können auf einem verwalteten Gerät überschrieben werden.

Die Anzahl der Einstellungen mit „Vorhängeschlössern“ in der Web Console und in der Verwaltungskonsole kann unterschiedlich sein.

Richtlinienprofil

Um zu vermeiden, dass eine große Anzahl von Richtlinien unterstützt werden muss, beispielsweise wenn nur wenige Einstellungen änderbar sein sollen, können Sie Richtlinienprofile verwenden.

Ein *Richtlinienprofil* ist eine Gruppe einzelner Richtlinieneinstellungen, die sich von den Einstellungen der „Basis“-Richtlinie unterscheiden und auf Client-Geräte angewendet werden, wenn die konfigurierten Bedingungen (Aktivierungsregeln) erfüllt sind. Die Verwendung von Richtlinienprofilen ermöglicht eine flexiblere Anpassung der Anwendungseinstellungen auf verschiedenen Geräten.

Die im Profil durch ein "Schloss" gesperrten Parameter haben eine höhere Priorität als Richtlinieneinstellungen. Wenn ein im Profil gesperrter Parameter also vom Richtlinienparameter abweicht, verwendet die Anwendung den Parameter aus dem Profil. Parameter, die in Listenform angezeigt werden, werden dabei zusammengeführt und ergänzen einander. Das heißt, wenn Parameter aus der Profilliste nicht in der "Basis"-Richtlinie vorhanden sind, werden sie der resultierenden Parameterliste hinzugefügt.

Für Richtlinienprofile gelten folgende Regeln:

- Ein Richtlinienprofil wird wirksam, wenn eine bestimmte Aktivierungsbedingung erfüllt ist.
- Richtlinienprofile enthalten Einstellungswerte, die sich von den in der Richtlinie festgelegten Werten unterscheiden.
- Durch die Aktivierung eines Richtlinienprofils werden die effektiven Einstellungen des verwalteten Geräts geändert (Einstellungen, die derzeit auf das Gerät angewendet werden).
- Eine Richtlinie kann bis zu 100 Profile haben.

Vererbung von Einstellungen

Genau wie Administrationsgruppen unterliegen auch Richtlinien einer Hierarchie. Eine *untergeordnete Richtlinie* ist eine Richtlinie der untergeordneten Hierarchieebene, d. h. eine Richtlinie für verschachtelte Administrationsgruppen und untergeordnete Administrationsserver.

Eine untergeordnete Richtlinie erbt standardmäßig die Einstellungen der übergeordneten Richtlinie. Wenn eine Einstellung in der übergeordneten Richtlinie gesperrt ist (🔒), erhalten untergeordnete Richtlinien und lokale Einstellungen des Programms denselben Wert, und die Einstellung ist gesperrt. Erforderlichenfalls können Sie die Vererbung von Einstellungen aus der übergeordneten Richtlinie deaktivieren. Mobile Richtlinien unterliegen nicht der Hierarchie von Administrationsgruppen für andere Richtlinien.

Wenn die Einstellungen der untergeordneten Richtlinie gesperrt sind (Fehler *Zugriff verweigert*), überprüfen Sie die Zugriffsrechte des Benutzers. Wenn der Benutzer berechtigt ist, Richtlinieneinstellungen zu ändern, starten Sie die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* für Kaspersky Security Center und wiederholen Sie die Autorisierung. Dieser Fehler kann nach dem Upgrade der Verwaltungs-Plug-ins in Kaspersky Security Center auftreten: Nach dem Herunterladen der Updates ruft das Programm die erforderlichen Dateien für die neue Version des Verwaltungs-Plug-ins ab.

Für einige Einstellungen, die Listen als Werte haben (z. B. Listen mit Regeln, Listen mit Ausnahmen), können Sie das Zusammenführen von Listenelementen aktivieren. Gehen Sie wie folgt vor, um Listenelemente zusammenzuführen:

- Aktivieren Sie in den Eigenschaften der untergeordneten Richtlinie auf der Registerkarte **Allgemein** die Einstellung **Einstellungen aus übergeordneter Richtlinie erben**.
- Sperren Sie in den Eigenschaften der übergeordneten Richtlinie die Liste anhand des "Schlosses" (🔒).
- Aktivieren Sie in den Eigenschaften der übergeordneten Richtlinie das Vereinigen von Einstellungen, indem Sie das Kontrollkästchen **Werte beim Vererben vereinen** aktivieren. Wenn das Kontrollkästchen aktiviert ist, werden die Listenelemente der übergeordneten Richtlinien von Kaspersky Security Center in den untergeordneten Richtlinien angezeigt und die Elemente können der Liste der untergeordneten Richtlinie hinzugefügt werden. Bei deaktiviertem Kontrollkästchen werden die Listenelemente beim Vererben von Richtlinieneinstellungen nicht vereinigt.

Sie können übernommene Listenelemente in einer untergeordneten Richtlinie weder löschen noch ändern. Die Elemente der Liste, die durch Vererbung vereinigt wurden, können nur in der übergeordneten Richtlinie gelöscht oder geändert werden. Das Hinzufügen, Ändern und Löschen von Elementen der Liste ist in untergeordneten Ebenen möglich. Auf diese Weise können Sie in einer übergeordneten Richtlinie eine Liste einrichten, die für alle untergeordneten Richtlinien gilt. Gleichzeitig können Sie die Liste in einer untergeordneten Richtlinie auch ergänzen.

Wenn Sie ein Element aus einer Liste löschen, die durch Vererbung in einer übergeordneten Richtlinie zusammengeführt wurde, wird dieses Element nicht aus den untergeordneten Richtlinien gelöscht. Um dieses Element aus den untergeordneten Richtlinien zu löschen, müssen Sie die Eigenschaften dieser Richtlinien öffnen und das Element manuell löschen.

Einige Listen werden nicht zusammengeführt. In diesem Fall überschreiben die Einstellungen aus dem Profil die Einstellungen der „Basis"-Richtlinie:

- Prozessbezogene Ausnahmen in den Komponenten Schutz vor Dateibedrohungen und Verhaltensanalyse
- Schutzbereich in den Komponenten Schutz vor bedrohlichen Dateien und Schutz vor Verschlüsselung
- Überwachungsbereiche in der Komponente Überwachung der System-Integrität
- Liste der Regeln (im Fenster **Regeln der Programmkontrolle**) in der Komponente Programmkontrolle
- Liste der Regeln in der Web-Kontrolle
- Untersuchungsausnahmen für Prozess-Speicher in den Anwendungseinstellungen
- vertrauenswürdige Domänen in den Netzwerkeinstellungen
- vertrauenswürdige Stammzertifikate in den Netzwerkeinstellungen
- überwachte Ports in den Netzwerkeinstellungen
- Liste der SVM-Adressen in den Einstellungen der SVM-Erkennung

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

Die Einstellungen einer zuvor gelöschten Richtlinie gelten weiterhin für das Gerät, bis es eine neue Richtlinie erhält oder die Einstellungen lokal auf dem Gerät geändert werden.

Weitere Informationen zu Richtlinien und Richtlinienprofilen sowie zum Mechanismus der Einstellungsvererbung finden Sie in der Hilfe zu Kaspersky Security Center.

Richtlinienverwaltung

So erstellen Sie eine Richtlinie in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

   Die Liste mit Richtlinien und Richtlinienprofilen wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, auf die Sie die Richtlinie anwenden möchten. Um eine verschachtelte Gruppe auszuwählen, klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Hierarchie anzeigen**.

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

   Der Assistent für neue Richtlinien wird gestartet.

4. Wählen Sie im neuen Fenster den Namen der Anwendung "Kaspersky Endpoint Security" aus.

   Wechseln Sie zum nächsten Schritt des Assistenten.

5. Geben Sie an, in welchem Modus Sie Kaspersky Endpoint Security verwenden:

   - In **Standard-Modus oder Endpoint Detection and Response Agent-Modus** wird die Anwendung zum Schutz von Linux-Geräten als eigenständige Anwendung oder als Anwendung verwendet, welche die gemeinsame Ausführung der Detection and Response-Lösungen von Kaspersky mit den Anti-Virus-Lösungen von Drittanbietern ermöglicht.

     Um diesen Modus auszuwählen, fahren Sie mit dem nächsten Schritt des Assistenten fort.

   - **Light Agent für den Schutz virtueller Umgebungen** – als Bestandteil der Lösung Kaspersky Security for Virtualization Light Agent wird die App zum Schutz virtueller Maschinen verwendet, auf denen Linux-Gastbetriebssysteme ausgeführt werden.

6. Wenn Sie die App im Light Agent-Modus 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.

      - **Benutzerdefinierte 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 **Benutzerdefinierte Liste mit SVM-Adressen verwenden** ausgewählt haben und für den Light Agent der erweiterte Algorithmus der SVM-Auswahl verwendet wird sowie auf einer SVM der Modus zum Schutz großer Infrastrukturen aktiviert ist, dann ist die Verbindung eines Light Agents mit dieser SVM nur möglich, wenn der Standort der SVM nicht berücksichtigt wird. Im Abschnitt **Algorithmus der SVM-Auswahl** müssen Sie die Einstellung **SVM-Standort** auf **Ignorieren** setzen. Bei einem beliebigen anderen angegebenen Wert kann der Light Agent keine Verbindung zur SVM herstellen. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

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 angezeigten Fenster neue Verbindungsparameter an:

      - **Adresse**. IP-Adresse im IPv4-Format oder als vollqualifizierter Domänenname (FQDN) des Geräts mit installiertem Integrationsserver. Wenn als Adresse ein NetBIOS-Name, localhost oder 127.0.0.1 angegeben ist, wird die Verbindung zum Integrationsserver mit einem Fehler beendet.

      - **Port**. Port für die Verbindung zum Integrationsserver. Der Standardport ist 7271.

      Wenn in Ihrer Infrastruktur ein Failover-Cluster von Integrationsservern auf Linux-Basis bereitgestellt ist, müssen Sie als Adresse und Port für die Verbindung zum Integrationsserver die Adresse und den Port des Load Balancers eingeben. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

   b. Klicken Sie auf die Schaltfläche **Überprüfen**.

   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 **Einstellungen der Verbindung zum Integrationsserver** eine entsprechende Meldung angezeigt.

      Sie können die Informationen über das vom Integrationsserver abgerufene Zertifikat anzeigen, indem Sie auf die Zeile **Empfangenes 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 **Maßnahme auswählen** die Option **Ignorieren** aus.

   d. Geben Sie das Administratorkennwort des Integrationsservers (Kennwort des Kontos `admin`) an und klicken Sie auf die Schaltfläche **Überprüfen**.

      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 **Eingerichtet** angezeigt.

c. Wenn Sie eine manuell definierte Liste mit SVM-Adressen auswählen, erstellen Sie eine Liste der SVMs, 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 mehrere IP-Adressen oder vollständige Domänennamen der 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 Anwendung 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 Bestimmungen der Erklärung einverstanden sind und Kaspersky Security Network mit der App verwenden möchten, wählen Sie **Ich akzeptiere die Nutzungsbedingungen für Kaspersky Security Network** aus.

   - Wenn Sie Kaspersky Security Network nicht verwenden möchten, wählen Sie **Ich lehne die Nutzungsbedingungen für Kaspersky Security Network ab** aus und bestätigen Sie Ihre Entscheidung im daraufhin geöffneten 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. Sie werden aufgefordert, die Empfehlungen zur Konfiguration von Kaspersky Endpoint Security zu lesen. Überprüfen Sie die Einstellungen, mit denen die App die Nutzung der Systemressourcen optimieren kann.

   Wechseln Sie zum nächsten Schritt des Assistenten.

9. 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. Dieser Status gilt als Standard.

     - **Inaktiv**. Wenn diese Option ausgewählt ist, wird die Richtlinie nicht auf das Gerät angewendet, verbleibt jedoch im Ordner **Richtlinien**. Später können Sie die inaktive Richtlinie aktivieren.

     - **Mobil**. Wenn diese Option ausgewählt ist, tritt die Richtlinie in Kraft, wenn das Gerät das Netzwerk der Organisation verlässt.

       In der Richtlinie des Administrationsagenten, die auf das Gerät angewendet wird, sollte im Abschnitt **Netzwerk → Verbindungsprofile** der Parameter **Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist** aktiviert sein.

- Vererbung von Richtlinieneinstellungen:

  - **Einstellungen aus übergeordneter Richtlinie übernehmen**. Wenn der Umschalter aktiviert ist, werden die Werte der Richtlinieneinstellung von der Gruppenrichtlinie höherer Ebene geerbt. Parameter, die in der übergeordneten Richtlinie durch das "Schloss" gesperrt sind (🔒), können nicht geändert werden. Der Schalter ist standardmäßig aktiviert.

  - **Vererbung von Einstellungen in untergeordneten Richtlinien erzwingen**. Wenn der Schalter aktiviert ist, werden die Richtlinieneinstellungen an untergeordnete Richtlinien weitervererbt. In den Eigenschaften der untergeordneten Richtlinie wird der Schalter **Einstellungen aus übergeordneter Richtlinie übernehmen** automatisch aktiviert und kann nicht mehr deaktiviert werden. Die Einstellungen der untergeordneten Richtlinie werden von der übergeordneten Richtlinie übernommen, außer bei Einstellungen, für die das "Schloss" geöffnet ist (🔓). Der Schalter ist standardmäßig deaktiviert.

  Allgemeine Informationen zu Richtlinieneinstellungen finden Sie in der Hilfe zu Kaspersky Security Center.

10. Wenn Sie andere Richtlinieneinstellungen verwalten möchten, wechseln Sie zur Registerkarte **App-Einstellungen** und nehmen Sie die erforderlichen Änderungen vor.

    Sie können die Richtlinieneinstellungen auch später ändern.

11. Klicken Sie auf **Speichern**.

So erstellen Sie eine Richtlinie in der Verwaltungskonsole

1. Wählen Sie in der Struktur der Verwaltungskonsole im Ordner **Verwaltete Geräte** die Administrationsgruppe aus, welche 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 den Namen der Anwendung "Kaspersky Security Center" 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 App-Version von Kaspersky Endpoint Security in die zu erstellende Richtlinie übertragen möchten, aktivieren Sie das Kontrollkästchen **Richtlinieneinstellungen einer früheren App-Version 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 Anwendung 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:

   - Im **Standard-Modus oder im Modus als Endpoint Detection and Response Agent** wird die Anwendung als entweder autonome Anwendung zum Schutz von Geräten mit Linux-Betriebssystemen oder als eine Anwendung verwendet, welche die gemeinsame Ausführung der Detection and Response-Lösungen von Kaspersky mit den Anti-Virus-Lösungen von Drittanbietern ermöglicht.

   - Im **Light Agent-Modus zum Schutz virtueller Umgebungen** wird die Anwendung 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 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.

      - **Benutzerdefinierte 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 **Benutzerdefinierte Liste mit SVM-Adressen verwenden** ausgewählt haben und für den Light Agent der erweiterte Algorithmus der SVM-Auswahl verwendet wird sowie auf einer SVM der Modus zum Schutz großer Infrastrukturen aktiviert ist, dann ist die Verbindung eines Light Agents mit dieser SVM nur möglich, wenn der Standort der SVM nicht berücksichtigt wird. Im Abschnitt **Algorithmus der SVM-Auswahl** müssen Sie die Einstellung **SVM-Standort** auf **Ignorieren** setzen. Bei einem beliebigen anderen angegebenen Wert kann der Light Agent keine Verbindung zur SVM herstellen. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

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 als Adresse ein NetBIOS-Name, localhost oder 127.0.0.1 angegeben ist, wird die Verbindung zum Integrationsserver mit einem Fehler beendet.

      - **Port**. Port für die Verbindung zum Integrationsserver. Der Standardport ist 7271.

      Wenn in Ihrer Infrastruktur ein Failover-Cluster von Integrationsservern auf Linux-Basis bereitgestellt ist, müssen Sie als Adresse und Port für die Verbindung zum Integrationsserver die Adresse und den Port des Load Balancers eingeben. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

   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 **Prüfung des Integrationsserver-Zertifikats** 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 eine manuell definierte Liste mit SVM-Adressen auswählen, erstellen Sie eine Liste der SVMs, 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 mehrere IP-Adressen oder vollständige Domänennamen der 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 Anwendung 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. Wählen Sie den Status der Richtlinie:

    - **Aktive Richtlinie**. 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. Dieser Status gilt als Standard.
    - **Inaktive Richtlinie**. Wenn diese Option ausgewählt ist, wird die Richtlinie nicht auf das Gerät angewendet, verbleibt jedoch im Ordner **Richtlinien**. Später können Sie die inaktive Richtlinie aktivieren.
    - **Richtlinie für mobile Benutzer**. Wenn diese Option ausgewählt ist, tritt die Richtlinie in Kraft, wenn das Gerät das Netzwerk der Organisation verlässt.

      In der Richtlinie des Administrationsagenten, die auf das Gerät angewendet wird, sollte im Abschnitt **Netzwerk → Verbindungsprofile** der Parameter **Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist** aktiviert sein.

15. 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.

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

Nützliche Artikel

Vorgehensweise, wenn Aufgaben nicht ausgeführt oder Richtlinien nicht angewendet werden

Vorgehensweise, wenn das Gerät den folgenden Status aufweist: „Ungültige Richtlinieneinstellungen. Richtlinie wurde nicht angewendet."

Fehler: „Die App wird von der aktuellen Version von Kaspersky Security Center Web Console nicht unterstützt oder das Web-Plug-in der App ist nicht installiert"

Exportieren und Importieren von Richtlinieneinstellungen

Mit Kaspersky Endpoint Security können Sie eine Richtlinie mit Einstellungen und Profilen in eine KLP-Datei exportieren. Anschließend können Sie die Export/Import-Funktion für Richtlinien verwenden, um ein Backup von Richtlinien anzulegen, Richtlinien auf einen anderen Server zu migrieren oder Richtlinien beispielsweise von Kaspersky Security Center Windows nach Kaspersky Security Center Linux zu migrieren. Details zur Verwaltung von Richtlinien finden Sie in der Hilfe zu Kaspersky Security Center.

So exportieren und importieren Sie eine Richtlinie (in der Verwaltungskonsole (MMC))

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu der die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. So exportieren Sie eine Richtlinie:
   a. Klicken Sie auf die Richtlinie, die Sie exportieren möchten.
   b. Klicken Sie auf den Link **Richtlinie in Datei exportieren**, der sich rechts im Fenster befindet.
   c. Geben Sie im folgenden Fenster den Namen der KLP-Datei an, in die Sie die Richtlinie exportieren möchten, und wählen Sie den Ordner aus, in dem die Datei gespeichert werden soll.
   d. Speichern Sie die Datei.
5. So importieren Sie eine Richtlinie:
   a. Klicken Sie auf **Richtlinie aus Datei importieren**.
   b. Wählen Sie im angezeigten Fenster die KLP-Richtliniendatei aus, die Sie importieren möchten.
   c. Öffnen Sie die Datei.

   Dadurch wird eine neue Richtlinie mit dem Status *Inaktive Richtlinie* hinzugefügt.

So exportieren und importieren Sie die Richtlinie in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. So exportieren Sie eine Richtlinie:
   a. Aktivieren Sie das Kontrollkästchen der Richtlinie, die Sie exportieren möchten.
   b. Klicken Sie auf die Schaltfläche **Exportieren**.
   c. Geben Sie im folgenden Fenster den Namen der KLP-Datei an, in die Sie die Richtlinie exportieren möchten, und wählen Sie den Ordner aus, in dem die Datei gespeichert werden soll.
   d. Speichern Sie die Datei.

3. So importieren Sie eine Richtlinie:

    a. Klicken Sie auf **Importieren**.

    b. Wählen Sie die KLP-Richtliniendatei aus, die Sie importieren möchten.

    c. Nachdem die Richtlinie erfolgreich verarbeitet wurde, wählen Sie die Administrationsgruppe aus, auf die Sie die Richtlinie anwenden möchten.

    d. Klicken Sie auf **Abgeschlossen**, um den Import der Richtlinie abzuschließen.

    Dadurch wird eine neue Richtlinie mit dem Status *Inaktiv* hinzugefügt.

Exportieren und Importieren bestimmter Richtlinieneinstellungen in der Web Console

In der Web Console können Sie einzelne Richtlinieneinstellungen in eine JSON-Datei exportieren und solche Einstellungen aus einer Datei importieren. Sie können beispielsweise eine Liste mit Regeln für die Web-Kontrolle oder Schutzbereiche für den Schutz vor bedrohlichen Dateien exportieren.

Die folgenden Einstellungen stehen für den Export und Import zur Verfügung:

- Schutzbereiche für den Schutz vor bedrohlichen Dateien
- Anhangsfilter von Schutz vor E-Mail-Bedrohungen
- Regeln für Netzwerkpakete
- Regeln für die Web-Kontrolle
- Regeln der Programmkontrolle
- Überwachungsbereiche und Ausnahmebereiche der Überwachung der Systemintegrität
- Telemetrie-Einstellungen
- Bestimmte Ausnahmen der Vertrauenswürdigen Zone

So exportieren oder importieren Sie Einstellungen in der Web Console:

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wechseln Sie zu dem Abschnitt, aus dem Sie Einstellungen exportieren oder importieren möchten.
5. Klicken Sie auf die Schaltfläche .

6. Wählen Sie eine Aktion aus: **Import** oder **Exportieren**.

7. Wenn Sie Einstellungen importieren, wählen Sie die Datei aus, aus der Sie die Einstellungen importieren möchten.

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 eine Geräteauswahl, die auf mehreren Geräten ausgeführt werden sollen, unabhängig von deren Zugehörigkeit zu Administrationsgruppen.

Sie können eine beliebige Anzahl von Aufgaben erstellen.

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

Typ der Aufgabe

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

- *Schadsoftware-Untersuchung*. Während der Ausführung dieser Aufgabe untersucht die Anwendung 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 vorhandene Viren und andere Schadsoftware.
- *Inventarisierung*. Während der Ausführung der Aufgabe ruft die App Informationen über alle ausführbaren Dateien ab, die auf den Geräten gespeichert sind, und verwaltet das Golden Image.
- *Überwachung der System-Integrität*. Während der Ausführung dieser Aufgabe registriert die Anwendung 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 Anwendung der aktive bzw. der Reserveschlüssel zur Aktivierung der Anwendung hinzugefügt.

- *Update*. Während der Ausführung dieser Aufgabe aktualisiert die Anwendung die Datenbanken entsprechend den festgelegten Update-Einstellungen.
- *Rollback des Datenbanken-Updates*. Während der Ausführung dieser Aufgabe führt die Anwendung ein Rollback des letzten Datenbanken-Updates durch.

Aufgabenverwaltung in Web Console

So erstellen Sie eine Aufgabe für eine Gruppe oder eine Geräteauswahl in der Web Console

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

   Die Aufgabenliste 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 Namen "Kaspersky Endpoint Security" aus.

   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 unmittelbar nach dem Erstellen der Aufgabe zu verwalten, aktivieren Sie im letzten Schritt des Assistenten das Kontrollkästchen **Aufgabendetails nach Abschluss der Erstellung öffnen**. Die Aufgabe wird mit Standardeinstellungen erstellt.

6. Schließen Sie den Assistenten ab.

Die neue Aufgabe wird in der Aufgabenliste angezeigt.

So erstellen Sie eine lokale Aufgabe in der Web Console

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 oberhalb der Liste der verwalteten Geräte auf die Schaltfläche **Hierarchie anzeigen** und wählen Sie im geöffneten Fenster eine 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 eine Aufgabe erstellen möchten, und klicken Sie auf den Gerätenamen.

4. Wechseln Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts zur Registerkarte **Aufgaben**.

   Eine Liste der für dieses Gerät erstellten Aufgaben wird geöffnet.

5. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

6. Gehen Sie im ersten Schritt des Assistenten folgendermaßen vor:

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

   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.

7. Um die Aufgabeneinstellungen unmittelbar nach dem Erstellen der Aufgabe zu verwalten, aktivieren Sie im letzten Schritt des Assistenten das Kontrollkästchen **Aufgabendetails nach Abschluss der Erstellung öffnen**. Die Aufgabe wird mit Standardeinstellungen erstellt.

8. Schließen Sie den Assistenten ab.

Die neue Aufgabe wird in der Aufgabenliste angezeigt.

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 Aufgabenliste 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 im oberen Teil des Fensters auf die Schaltfläche **Hierarchie anzeigen** 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 Geräteauswahl), klicken Sie im oberen Teil des Fensters auf die Schaltfläche **Hierarchie anzeigen** und wählen Sie im angezeigten Fenster den obersten Knoten mit dem Namen des Administrationsservers aus.

     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.

> Die *Update-Aufgabe* kann nicht angehalten oder fortgesetzt werden; sie kann nur gestartet und beendet werden.

Aufgaben in der Verwaltungskonsole verwalten

So erstellen Sie in der Verwaltungskonsole eine Aufgabe für eine Gruppe oder eine Geräteauswahl

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 den Namen der Anwendung "Kaspersky Endpoint Security" 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 Informationen 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, welche 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. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

So erstellen Sie eine lokale Aufgabe in der Verwaltungskonsole

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 **Aufgaben** aus.

   Eine Liste der für dieses Gerät erstellten Aufgaben wird geöffnet.

5. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

6. Wählen Sie im ersten Schritt des Assistenten den Namen der Anwendung "Kaspersky Endpoint Security" und den Aufgabentyp aus.

   Wechseln Sie zum nächsten Schritt des Assistenten.

7. Geben Sie den Namen der neuen Aufgabe ein und folgen Sie den Anweisungen des Assistenten, um die Aufgabeneinstellungen zu konfigurieren.

8. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

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.

   Die *Update-Aufgabe* kann nicht angehalten oder fortgesetzt werden; sie kann nur gestartet und beendet werden.

In der Liste der Aufgaben können Sie die Aufgabenausführung überwachen, indem Sie den Aufgabenstatus und die Statistik zur Aufgabenausführung auf den Geräten anzeigen. Sie können auch eine Auswahl von Ereignissen erstellen, um die Ausführung von Aufgaben zu überwachen. Weitere Informationen über die Ereignisauswahl finden Sie in der Hilfe zu Kaspersky Security Center.

Die Ergebnisse der Aufgabenausführung werden auch lokal auf dem Gerät und in den Berichten von Kaspersky Security Center gespeichert.

Besonderheiten bei der Verwaltung und Ausführung von Aufgaben

- Die Aufgabe für Geräteauswahlen wird nur auf den Geräten ausgeführt, die in der Aufgabe angegeben sind. Wenn der Geräteauswahl, für die eine Aufgabe erstellt wurde, neue Geräte hinzugefügt werden, wird diese Aufgabe für diese Geräte nicht ausgeführt. In diesem Fall müssen Sie eine neue Aufgabe erstellen oder die vorhandene Aufgabe bearbeiten.

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

- Wenn das Gerät durch eine Richtlinie verwaltet wird, können in Kaspersky Security Center erstellte Aufgaben möglicherweise nicht über die Befehlszeile oder die grafische Oberfläche der Anwendung angezeigt und verwaltet werden.

- Für das Programm Kaspersky Endpoint Security in Kaspersky Security Center können Sie alle Arten von Aufgaben erstellen. Das Anwenden und Ausführen von Aufgaben auf einem geschützten Gerät wird durch den Modus des Programms auf dem Gerät bestimmt. So werden beispielsweise die Aufgaben *Schlüssel hinzufügen*, *Update* und *Rollback des Datenbanken-Updates* nicht auf dem Gerät angewendet, wenn das Programm im Light Agent-Modus ausgeführt wird.

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.

Sie können sich mit einer der folgenden Methoden an der Kaspersky Security Center Web Console anmelden:

- Domänenauthentifizierung (Single Sign-On)

- Benutzername und Kennwort eines Domänenbenutzers

- Benutzername und Kennwort eines internen Benutzers

Weitere Informationen zur An- und Abmeldung bei der Kaspersky Security Center Web Console finden Sie in der Hilfe zu Kaspersky Security Center.

So melden Sie sich durch Angabe von Benutzername und Kennwort bei der Web Console an:

1. Rufen Sie in Ihrem Browser folgende Adresse auf:

   ```
   https://<Kaspersky Security Center Web Console address>:<port number>
   ```

   Die Seite zur Auswahl des Administrationsservers wird geöffnet.

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

   Wenn Sie nur einen Administrationsserver hinzugefügt haben, wird die Liste der Administrationsserver nicht angezeigt.

   Der Browser wird zu `https://<Administration Server address>:4444` umgeleitet.

3. 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.

4. Klicken Sie auf **Anmelden**.

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

5. Geben Sie den einmaligen Sicherheitscode ein, der in der Authentifizierungs-App auf Ihrem mobilen Gerät generiert wurde.

   Wenn Sie sich zum ersten Mal anmelden, konfigurieren Sie die 2-Schritt-Authentifizierung für Ihr Konto.

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

Weitere Informationen zur Benutzeroberfläche der Web Console finden Sie in der Hilfe 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.

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

App über die Befehlszeile verwalten

Über die Befehlszeile können Sie Kaspersky Endpoint Security auf dem Gerät installieren, deinstallieren, starten und beenden sowie das Programm lokal verwalten.

Komponenten und Aufgaben

Die Ausführung der Funktionskomponenten der Anwendung wird durch *lokale Aufgaben von Kaspersky Endpoint Security* sichergestellt, die im Betriebssystem ausgeführt werden Um eine Funktionskomponente des Programms auf einem Gerät zu aktivieren oder zu deaktivieren, müssen Sie in der Befehlszeile die entsprechende Aufgabe von Kaspersky Endpoint Security starten oder beenden.

Um ein Gerät einmalig zu untersuchen, müssen Sie ebenfalls die entsprechende Aufgabe von Kaspersky Endpoint Security starten.

Um die Einstellungen einer Funktionskomponente auf einem Gerät oder die Einstellungen für die Untersuchung eines Geräts zu verwalten, müssen Sie die Einstellungen der entsprechenden Aufgabe von Kaspersky Endpoint Security verwalten.

Allgemeine Einstellungen

Neben den Einstellungen, die für einzelne Aufgaben von Kaspersky Endpoint Security spezifisch sind, gibt es einige allgemeine Einstellungen:

- Allgemeine Einstellungen der Untersuchung von Containern. Wird bei der Echtzeit-Untersuchung von Containern und Namespaces verwendet (Container-Überwachung).
- Einstellungen der Untersuchung des Netzwerkdatenverkehrs. Wird von den Komponenten Schutz vor Web-Bedrohungen, Schutz vor Netzwerkbedrohungen, Schutz vor E-Mail-Bedrohungen und Web-Kontrolle verwendet.
- Allgemeine Programmeinstellungen. Diese Einstellungen bestimmen die Funktionsweise des Programms als Ganzes und einzelner Funktionen.

Verwaltungsbefehle

Sie können Aufgaben und Einstellungen von Kaspersky Endpoint Security über die Befehlszeile mithilfe der *kesl-control-Dienstprogramme* verwalten.

Es können nur Benutzeraufgaben erstellt oder gelöscht werden. Vordefinierte Aufgaben können nicht erstellt oder gelöscht werden.

Je nach Modus des Programms können Sie die folgenden Arten von Benutzeraufgaben erstellen:

- Im Standard-Modus: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* und *InventoryScan*.
- Light Agent-Modus: *ODS*, *ODFIM*, *ContainerScan* und *InventoryScan*.

Sie können alle vordefinierten Aufgaben und Benutzeraufgaben starten und beenden, mit Ausnahme von Aufgaben des Typs *License*.

Sie können *ODS*-, *ODFIM*- und *InventoryScan*-Aufgaben anhalten und fortsetzen.

Lokale Aufgaben von Kaspersky Endpoint Security

Für die Verwaltung von Kaspersky Endpoint Security über die Befehlszeile können die folgenden Aufgaben verwendet werden, die in der folgenden Tabelle aufgeführt sind:

Jede Programmaufgabe hat einen Namen, der in der Befehlszeile verwendet wird, eine ID und einen Typ.

IDs sind für alle Aufgaben eindeutig, auch für Remote-Aufgaben. Die Anwendung 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 Installation der Anwendung 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 Anwendung erstellen, werden als *Benutzeraufgaben* bezeichnet. Die Namen dieser Aufgaben geben Sie beim Erstellen einer Aufgabe an. Die Anwendung definiert und weist einer Aufgabe Benutzeraufgaben-IDs zu, wenn diese erstellt wird. Die IDs für Benutzeraufgaben beginnen bei 100.

Während der Ausführung der Anwendung erstellt diese *temporäre Aufgaben zur Untersuchung*. Die Namen und IDs temporärer Aufgaben werden von der Anwendung festgelegt. Temporäre Aufgaben werden nach Abschluss automatisch gelöscht.

Aufgaben der Anwendung

Aufgabe	Aufgabenbeschreibung	Aufgabenname in der Befehlszeile	Aufgaben-ID	Aufgabentyp
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. Wenn der Schutz vor bedrohlichen Dateien aktiviert ist, wird die Aufgabe beim Programmstart automatisch ausgeführt	File_Threat_Protection	1	OAS
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.	Scan_My_Computer	2	ODS
Schadsoftware-Untersuchung (benutzerdefiniert)		Benutzereingabe	ab 100	ODS
Benutzerdefinierte Untersuchung von Dateien	Mit dieser Aufgabe können Sie Einstellungen konfigurieren und speichern, die bei der Untersuchung der angegebenen 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.	Scan_File	3	ODS
Untersuchung wichtiger Bereiche.	Mit dieser Aufgabe können Sie Untersuchung kritischer Bereiche des Betriebssystems auf Befehl ausführen und Einstellungen für die Untersuchung definieren.	Critical_Areas_Scan	4	ODS
Update	Mit dieser Aufgabe können Sie die Aktualisierung der Datenbanken und Module der Anwendung nach Zeitplan oder bei Bedarf ausführen und Update-Einstellungen konfigurieren.	Update	6	Update
Update (benutzerdefiniert)		Benutzereingabe	ab 100	Update
Rollback.	Mit dieser Aufgabe können Sie ein Rollback des letzten Updates der Programmdatenbanken und -module durchführen.	Rollback	7	Rollback
Rollback des Datenbanken-Updates (benutzerdefiniert)		Benutzereingabe	ab 100	Rollback
Lizenzverwaltung	Mit dieser Aufgabe können Sie eine auf dem Gerät installierte Anwendung aktivieren. Die Aufgabe startet automatisch beim Start der Anwendung 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.	License	9	License

Aufgabe	Aufgabenbeschreibung	Aufgabenname in der Befehlszeile	Aufgaben-ID	Aufgabentyp
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.	System_Integrity_Monitoring	11	OAFIM
Prüfung der Systemintegrität (Benutzeraufgabe)		Benutzereingabe	ab 100	ODFIM
Firewall-Verwaltung	Mit dieser Aufgabe können Sie die Firewall-Verwaltung aktivieren und deaktivieren und Einstellungen für die Überwachung von Netzwerkverbindungen auf dem Gerät definieren.	Firewall_Management	12	Firewall
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.	Anti_Cryptor	13	AntiCryptor
Schutz vor Web-Bedrohungen	Mit dieser Aufgabe können Sie den Schutz vor Web-Bedrohungen aktivieren oder deaktivieren und die Einstellungen für die Komponente Schutz vor Web-Bedrohungen festlegen. Wenn der Schutz vor Web-Bedrohungen aktiviert ist, wird die Aufgabe beim Programmstart automatisch ausgeführt	Web_Threat_Protection	14	WTP
Gerätekontrolle	Mit dieser Aufgabe können Sie die Gerätekontrolle aktivieren und deaktivieren und Einstellungen für die Komponente "Gerätekontrolle" definieren. Wenn die Gerätekontrolle aktiviert ist, wird die Aufgabe beim Programmstart automatisch ausgeführt.	Device_Control	15	DeviceControl
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.	Removable_Drives_Scan	16	RDS
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.	Network_Threat_Protection	17	NTP
Container untersuchen	Mit dieser Aufgabe können Sie Untersuchung von Container und Images auf Befehl ausführen und Einstellungen für die Untersuchung definieren.	Container_Scan	18	ContainerScan
Untersuchung von Containern (benutzerdefiniert)		Benutzereingabe	ab 100	ContainerScan
Benutzerdefinierte Untersuchung von Containern	Mit dieser Aufgabe können Sie Einstellungen konfigurieren und speichern, die bei der Untersuchung der angegebenen 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.	Custom_Container_Scan	19	ContainerScan

Aufgabe	Aufgabenbeschreibung	Aufgabenname in der Befehlszeile	Aufgaben-ID	Aufgabentyp
Verhaltensanalyse	Mit dieser Aufgabe können Sie schädliche Aktivitäten von Anwendungen im Betriebssystem überwachen. Wenn die Verhaltensanalyse aktiviert ist, wird die Aufgabe beim Programmstart automatisch ausgeführt.	Behavior_Detection	20	BehaviorDetection
Programmkontrolle	Mit dieser Aufgabe können Sie die Programmkontrolle aktivieren und deaktivieren und Einstellungen für die Komponente "Programmkontrolle" definieren.	Application_Control	21	AppControl
Inventarisierung	Mit dieser Aufgabe ist das Abrufen von Informationen über alle ausführbaren Dateien von Programmen auf dem Gerät sowie die Verwaltung der Programmkategorie „Golden Image" möglich.	Inventory_Scan	22	InventoryScan
Inventarisierung (benutzerdefiniert)		Benutzereingabe	ab 100	InventoryScan
Integration in Kaspersky Endpoint Detection and Response Expert (on-premises).	Mit dieser Aufgabe können Sie die Integration in Kaspersky Endpoint Detection and Response Expert (on-premises) oder in Kaspersky Endpoint Detection and Response (KATA) aktivieren oder deaktivieren und Integrationseinstellungen verwalten.	KATAEDR	24	KATAEDR
Web-Kontrolle	Mit dieser Aufgabe können Sie die Web-Kontrolle aktivieren und deaktivieren und Einstellungen für die Komponente "Web-Kontrolle" definieren.	Web_Control	26	WebControl
Integration mit Sandbox	Mit dieser Aufgabe können Sie die Integration der Komponente Sandbox aktivieren und deaktivieren sowie die Integrationseinstellungen festlegen.	Standalone_Sandbox	29	StandaloneSandbox
Ausführungsprävention für Objekte (EDR Expert (on-premise))	Mit dieser Aufgabe können Sie die Verwendung von Regeln für die Ausführungsprävention von Endpoint Detection and Response Expert (on-premise) aktivieren und deaktivieren sowie eine Liste dieser Regeln anzeigen.	KATAEDR_Prevention	30	KATAEDRPrevention
Integration mit Kaspersky Network Detection and Response (KATA).	Mit dieser Aufgabe können Sie die Integration mit Kaspersky Network Detection and Response (KATA) aktivieren und deaktivieren und Integrationseinstellungen festlegen.	KATANDR	31	KATANDR
Ausführungsprävention für Objekte (EDR Optimum)	Mit dieser Aufgabe können Sie die Verwendung der Regeln von Endpoint Detection and Response Optimum zur Ausführungsprävention für Objekte aktivieren und deaktivieren sowie eine Liste dieser Regeln anzeigen.	EDRO_Prevention	32	Prevention
Integration mit KUMA	Mit dieser Aufgabe können Sie die Integration mit Kaspersky Unified Monitoring and Analysis Platform aktivieren und deaktivieren sowie die Integrationseinstellungen festlegen.	KUMA	33	KUMA

Aufgabe	Aufgabenbeschreibung	Aufgabenname in der Befehlszeile	Aufgaben-ID	Aufgabentyp
Schutz vor E-Mail-Bedrohungen	Mit dieser Aufgabe können Sie eine Untersuchung der Anhänge eingehender und ausgehender E-Mail-Nachrichten auf Viren und andere bedrohliche Programme durchführen. Wenn der Schutz vor E-Mail-Bedrohungen aktiviert ist, wird die Aufgabe beim Programmstart automatisch ausgeführt	Mail_Monitoring	35	MailMonitoring
Schutz vor BadUSB-Angriffen	Mit dieser Aufgabe können Sie verhindern, dass infizierte USB-Geräte, die eine Tastatur imitieren, mit einem Client-Gerät verbunden werden.	Bad_USB	37	BadUSB
Integration in Kaspersky Endpoint Detection and Response Expert (cloud)	Mit dieser Aufgabe können Sie die Integration in Kaspersky Endpoint Detection and Response Expert (cloud) aktivieren oder deaktivieren und die Integrationseinstellungen festlegen.	EDRExpertCloud	39	EDRExpertCloud

Aufgabenparameter ändern

Sie können die Einstellungen aller Benutzeraufgaben und aller vordefinierten Aufgaben ändern, mit Ausnahme von Aufgaben der Typen *Rollback* und *License* (diese Aufgaben haben keine Einstellungen). Wenn das Programm im Light Agent-Modus verwendet wird, können die Einstellungen der vordefinierten Aufgabe *Update* ebenfalls nicht geändert werden.

Für Aufgaben der Typen *OAS*, *ODS*, *OAFIM*, *ODFIM* und *AntiCryptor* können Sie Untersuchungsbereiche und Ausschlussbereiche hinzufügen oder entfernen.

Sie können die Aufgabeneinstellungen auf folgende Weise ändern:

- Mithilfe einer Konfigurationsdatei. Mit dieser Methode können alle Aufgabeneinstellungen gleichzeitig geändert werden. Sie können die zu bearbeitende Konfigurationsdatei mit dem Befehl abrufen, der die Aufgabeneinstellungen ausgibt.

- Mithilfe von Befehlszeilenoptionen im Format <Einstellungsname>=<Einstellungswert>. Mit dieser Methode können einzelne Aufgabeneinstellungen geändert werden. Sie können die aktuellen Werte der Aufgabeneinstellungen mit dem Befehl anzeigen, der die Aufgabeneinstellungen ausgibt.

Einige Aufgaben verfügen auch über separate Verwaltungsbefehle, mit denen Sie Aufgabeneinstellungen ändern können.

So geben Sie die aktuellen Werte der Aufgabeneinstellungen aus

Sie können die aktuellen Werte der Aufgabeneinstellungen in die Konsole oder in eine Konfigurationsdatei ausgeben. Anschließend können Sie diese Datei bearbeiten, um die Aufgabeneinstellungen zu ändern.

```
Aktuelle Werte der Aufgabeneinstellungen in die Konsole ausgeben

kesl-control --get-settings <task ID|name>
```

Wobei gilt:

- `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

```
Aktuelle Werte der Aufgabeneinstellungen in eine Konfigurationsdatei ausgeben

kesl-control --get-settings <task ID/name> --file <path to configuration file> [--json]
```

Wobei gilt:

- `--file <path to configuration file>` ist der Pfad zur Konfigurationsdatei, in die Sie die Aufgabeneinstellungen ausgeben möchten. 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.

So ändern Sie Aufgabeneinstellungen mithilfe einer Konfigurationsdatei:

1. Geben Sie die Aufgabeneinstellungen mit folgendem Befehl in die Konfigurationsdatei aus:

   ```
   kesl-control --get-settings --file <path to configuration file> [--json]
   ```

   wobei:

   - `--file <path to configuration file>` ist der vollständige Pfad zur Konfigurationsdatei, aus der Sie die Aufgabeneinstellungen importieren möchten.

   - Geben Sie die Option `--json` an, wenn Sie die Einstellungen in eine Konfigurationsdatei im JSON-Format ausgeben möchten. Wenn die Option `--json` nicht angegeben ist, gibt die Anwendung die Einstellungen in eine Datei im INI-Format aus.

2. Öffnen Sie die resultierende Konfigurationsdatei, ändern Sie die Einstellungen nach Bedarf und speichern Sie Ihre Änderungen.

   Für Aufgaben der Typen *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` ist der Pfad zum Verzeichnis mit den zu untersuchenden 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` ist der Pfad zum Verzeichnis mit den auszuschließenden 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. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control --set-settings <task ID/name> --file <path to configuration file> [--json]
   ```

   wobei:

   - `<task ID/name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
   - `--file <path to configuration file>` ist der vollständige Pfad zur Konfigurationsdatei, aus der Sie die Aufgabeneinstellungen importieren möchten.
   - `--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 Anwendung, 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 Anwendung importiert.

Wenn Sie in den Einstellungen der Aufgabe Programmkontrolle die Liste mit erlaubten Anwendungen ändern oder den Start aller Anwendungen und/oder der Anwendungen, welche die Ausführung von Kaspersky Endpoint Security beeinflussen, verbieten, müssen Sie den Befehl `--set-settings` mit dem Schalter `--accept` ausführen.

So ändern Sie einzelne Aufgabeneinstellungen mithilfe von Befehlszeilenoptionen

Führen Sie den Befehl aus:

```
kesl-control --set-settings <task ID|name> <setting name >=<setting value> [<setting name >=<setting value>]
```

Wobei gilt:

- `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `<setting name >=<setting value>` ist der Name und der Wert einer Aufgabeneinstellung. Sie können die aktuellen Werte der Aufgabeneinstellungen mit dem Befehl zur Anzeige der Aufgabeneinstellungen abrufen.

Die Werte der angegebenen Aufgabeneinstellungen werden geändert.

Wenn Sie in den Einstellungen der Aufgabe Programmkontrolle die Liste mit erlaubten Anwendungen ändern oder den Start aller Anwendungen und/oder der Anwendungen, welche die Ausführung von Kaspersky Endpoint Security beeinflussen, verbieten, müssen Sie den Befehl `--set-settings` mit dem Schalter `--accept` ausführen.

So fügen Sie mithilfe von Befehlszeilenoptionen einen Untersuchungsbereich hinzu oder entfernen ihn

```
Einen Untersuchungsbereich mithilfe von Befehlszeilenoptionen hinzufügen
```

```
kesl-control --set-settings <task ID|name> --add-path <path>
```

Wobei gilt:

- `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `<path>` ist der Pfad zum Verzeichnis mit den zu untersuchenden Objekten.

Dieser Befehl fügt den Aufgabeneinstellungen einen neuen Abschnitt vom Typ `[ScanScope.item_#]` hinzu. Die Anwendung 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 `Path` 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 für das Hinzufügen des Verzeichnisses /home zum Untersuchungsbereich für eine Aufgabe mit ID=100
```

```
kesl-control --set-settings 100 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/home
```

Die folgenden Einstellungen für den Untersuchungsbereich werden der Aufgabe hinzugefügt:

```
[ScanScope.item_0001]
AreaDesc=
UseScanArea=Yes
```

```
Path=/home
AreaMask.item_0000=*
```

Einen Untersuchungsbereich mithilfe von Befehlszeilenoptionen entfernen

```
kesl-control --set-settings <task ID|name> --del-path <path>
```

Dieser Befehl entfernt den Abschnitt `[ScanScope.item_#]`, der den angegebenen Pfad enthält, aus den Aufgabeneinstellungen. Die App untersucht keine der Objekte im angegebenen Verzeichnis.

So fügen Sie mithilfe von Befehlszeilenoptionen einen Ausschlussbereich hinzu oder entfernen ihn

Einen Ausschlussbereich mithilfe von Befehlszeilenoptionen hinzufügen

```
kesl-control --set-settings <task ID|name> --add-exclusion <path>
```

Wobei gilt:

- `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `<path>` ist der Pfad zum Verzeichnis mit den auszuschließenden Objekten.

Dieser Befehl fügt den Aufgabeneinstellungen einen neuen Abschnitt vom Typ `[ExcludedFromScanScope.item_#]` hinzu. Die App schließt die Objekte in dem Verzeichnis, das durch die Einstellung `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 `Path` 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.

Einen Ausschlussbereich mithilfe von Befehlszeilenoptionen entfernen

```
kesl-control --set-settings <task ID|name> --del-exclusion <path>
```

Dieser Befehl entfernt den Abschnitt `[ExcludedFromScanScope.item_#]`, der den angegebenen Pfad enthält, aus den Aufgabeneinstellungen. Die App schließt keines der Objekte im angegebenen Verzeichnis von der Untersuchung aus.

So stellen Sie die standardmäßigen Aufgabeneinstellungen wieder her

Führen Sie den Befehl aus:

```
kesl-control --set-settings <task ID|name> --set-to-default
```

Dabei ist `<task ID|name>` die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Die Anwendung setzt die Werte der Einstellungen auf die Standardwerte zurück.

Zeitplan für Aufgaben konfigurieren

Je nach Modus des Programms können Sie einen Zeitplan für die folgenden Aufgabentypen konfigurieren:

- Im Standard-Modus: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* und *InventoryScan*.
- Light Agent-Modus: *ODS*, *ODFIM*, *ContainerScan* und *InventoryScan*.

Sie können den Aufgabenzeitplan auf folgende Arten ändern:

- Mithilfe einer Konfigurationsdatei. Mit dieser Methode können Sie alle Einstellungen des Aufgabenzeitplans gleichzeitig ändern. Sie können eine Konfigurationsdatei zur Bearbeitung mithilfe des Befehls abrufen, mit dem die Zeitplaneinstellungen ausgegeben werden.
- Mithilfe von Befehlszeilenoptionen im Format <Einstellungsname>=<Einstellungswert>. Mit dieser Methode können Sie einzelne Einstellungen des Aufgabenzeitplans ändern. Sie können die aktuellen Werte der Aufgabeneinstellungen mithilfe des Befehls anzeigen, mit dem die Zeitplaneinstellungen ausgegeben werden.

So geben Sie die aktuellen Zeitplaneinstellungen aus

Sie können die aktuellen Werte für die Einstellungen des Zeitplans für den Aufgabenstart in die Konsole oder in eine Konfigurationsdatei ausgeben. Anschließend können Sie diese Datei bearbeiten, um die Einstellungen zu ändern.

Aktuelle Einstellungen des Aufgabenzeitplans in die Konsole ausgeben

```
kesl-control --get-schedule <task ID|name> [--json]
```

Wobei gilt:

- `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie das Argument "--json" nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Aktuelle Einstellungen des Aufgabenzeitplans in eine Konfigurationsdatei ausgeben

```
kesl-control --get-schedule <task ID|name> --file <path to configuration file> [--json]
```

Dabei ist `--file <path to configuration file>` der Pfad zur Konfigurationsdatei, in die Sie die Einstellungen des Aufgabenzeitplans ausgeben möchten. 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.

Beispiel für die Ausgabe der Zeitplaneinstellungen der Update-Aufgabe in eine Datei mit dem Namen update_schedule.ini und das Speichern der erstellten Datei im aktuellen Verzeichnis

```
kesl-control --get-schedule 6 --file update_schedule.ini
```

Beispiel für die Ausgabe des Zeitplans der Update-Aufgabe im Terminal

```
kesl-control --get-schedule 6
```

So konfigurieren Sie den Aufgabenzeitplan mithilfe einer Konfigurationsdatei

```
kesl-control --set-schedule <task ID|name> --file <path to configuration file> [--json]
```

Wobei gilt:

- `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--file <path to configuration file>` ist der vollständige Pfad zur Konfigurationsdatei, aus der Sie die Einstellungen des Aufgabenzeitplans importieren möchten.
- `--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 Anwendung, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

```
Beispiel für den Import von Zeitplaneinstellungen aus der Konfigurationsdatei /home/test/on_demand_schedule.ini in die Aufgabe mit ID=2
```

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

So ändern Sie die Einstellungen des Aufgabenzeitplans mithilfe von Befehlszeilenoptionen:

```
kesl-control --set-schedule <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

Wobei gilt:

- `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `<setting name>=<setting value>` ist der Name und der Wert einer Einstellung des Aufgabenzeitplans.

```
Beispiel für die Konfiguration einer Aufgabe, die alle 10 Stunden ausgeführt wird
```

```
RuleType=Hourly
RunMissedStartRules=No
StartTime=2021/May/30 23:05:00;10
RandomInterval=0
```

```
Beispiel für die Konfiguration einer Aufgabe, die alle 10 Minuten ausgeführt wird
```

```
RuleType=Minutely
RunMissedStartRules=No
StartTime=23:10:00;10
RandomInterval=0
```

```
Beispiel für die Konfiguration einer Aufgabe, die am 15. jedes Monats ausgeführt wird
```

```
RuleType=Monthly
RunMissedStartRules=No
StartTime=23:25:00;15
RandomInterval=0
```

```
Beispiel für die Konfiguration einer Aufgabe, die jeden Dienstag ausgeführt wird
```

```
RuleType=Weekly
StartTime=18:01:30;Tue
```

```
RandomInterval=99
RunMissedStartRules=No
```

Beispiel für die Konfiguration einer Aufgabe, die alle 11 Tage ausgeführt wird

```
RuleType=Daily
RunMissedStartRules=No
StartTime=23:15:00;11
RandomInterval=0
```

Allgemeine App-Einstellungen verwalten

Die allgemeinen Anwendungseinstellungen bestimmen die Ausführung der Anwendung als Ganzes und die Ausführung einzelner Funktionen. Mit den allgemeinen Einstellungen können Sie Folgendes tun:

- Konfigurieren Sie die Verwendung von Kaspersky Security Network und die Light-Version der Anti-Malware-Datenbanken in der App.
- Konfigurieren Sie die Verwendung eines Proxy-Servers in der Anwendung.
- Konfigurieren Sie den Modus des Interceptors von Dateioperationen (Dateien während der Untersuchung blockieren/nicht blockieren).
- Konfigurieren Sie Ausschlüsse von der Untersuchung von Mountpunkten (globale Ausschlüsse).
- Konfigurieren Sie Ausnahmen von der Untersuchung des Prozessspeichers.
- Aktivieren oder deaktivieren Sie die Container-Überwachung in Echtzeit.
- Aktivieren und deaktivieren Sie die Erkennung von legitimen Anwendungen, 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 durch Untersuchungsaufgaben (vom Typ ODS).
- Begrenzen Sie die Anzahl der benutzerdefinierten Untersuchungsaufgaben, die ein nicht privilegierter Benutzer gleichzeitig ausführen kann.

Sie können allgemeine App-Einstellungen mithilfe von speziellen Verwaltungsbefehlen auf folgende Weise verwalten:

- Mithilfe einer Konfigurationsdatei. Mit dieser Methode können alle allgemeinen Einstellungen gleichzeitig geändert werden. Sie können mithilfe des Befehls zur Ausgabe der allgemeinen Einstellungen eine Konfigurationsdatei zur Bearbeitung abrufen.
- Mithilfe von Befehlszeilenoptionen im Format <Einstellungsname>=<Einstellungswert>. Mit dieser Methode können einzelne Einstellungen geändert werden. Sie können die aktuellen Werte der Einstellungen mithilfe des Befehls zur Ausgabe der allgemeinen Einstellungen abrufen.

So geben Sie die aktuellen Werte der allgemeinen Programmeinstellungen aus

Sie können die aktuellen Werte der allgemeinen App-Einstellungen in die Konsole oder in eine Konfigurationsdatei ausgeben. Anschließend können Sie mit dieser Datei die Einstellungen ändern.

Aktuelle Werte der allgemeinen Einstellungen der App in der Konsole ausgeben

```
kesl-control --get-app-settings [--json]
```

Dabei wird `--json` angegeben, um die Einstellungen im JSON-Format auszugeben. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Aktuelle Werte der allgemeinen Einstellungen der App in eine Konfigurationsdatei ausgeben

```
kesl-control --get-app-settings --file <path to configuration file> [--json]
```

Dabei ist `--file <path to configuration file>` der Pfad zur Konfigurationsdatei, in die Sie die allgemeinen Einstellungen der App ausgeben möchten. 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.

Beispiel für das Schreiben allgemeiner Programmeinstellungen in die Datei kesl_config.ini im aktuellen Verzeichnis

```
kesl-control --get-app-settings --file kesl_config.ini
```

So bearbeiten Sie Aufgabeneinstellungen mithilfe einer Konfigurationsdatei:

1. Geben Sie die allgemeinen App-Einstellungen mithilfe des Befehls `kesl-control --get-app-settings` in eine Konfigurationsdatei aus.

2. Öffnen Sie die resultierende Konfigurationsdatei, ändern Sie die Einstellungen nach Bedarf und speichern Sie Ihre Änderungen.

3. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control --set-app-settings --file <path to configuration file> [--json]
   ```

   wobei:

   - `--file <path to configuration file>` ist der vollständige Pfad zur Konfigurationsdatei mit den allgemeinen App-Einstellungen. Wenn Sie einen beliebigen Parameter in der Konfigurationsdatei löschen, wird nach Ausführung des Befehls der Standardwert für diesen Parameter zugewiesen.

   - `--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 Anwendung, 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 Anwendung importiert.

Beispiel für den Import allgemeiner Einstellungen aus der Konfigurationsdatei /home/test/kesl_config.ini in das Programm

```
kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

So ändern Sie allgemeine Einstellungen mithilfe von Befehlszeilenoptionen

Ändern Sie allgemeine Einstellungen mithilfe von Befehlszeilenoptionen

```
kesl-control --set-app-settings <setting name>=<setting value> [<setting name >=<setting value>]
```

Dabei ist `<setting name>=<setting value>` der Name und der Wert einer allgemeinen App-Einstellung.

Die Werte der angegebenen allgemeinen Einstellungen werden geändert.

Beispiel für die Einstellung einer niedrigen Detailstufe für die Protokolldatei

```
kesl-control --set-app-settings TraceLevel=NotDetailed
```

Beispiel für das Hinzufügen einer Ausnahme für einen Einhängepunkt vom Abfangen von Dateivorgängen

```
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 Anwendungsverwaltung eingrenzen. Filterbedingungen werden mithilfe eines oder mehrerer *logischer Ausdrücke* angegeben, die mit dem logischen Operator `and` kombiniert werden. Filterbedingungen müssen in Anführungszeichen gesetzt werden:

Sie können einen Filter für folgende Zwecke verwenden:

Informationen zu bestimmten aktuellen App-Ereignissen anzeigen

```
kesl-control -W --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

Informationen zu bestimmten App-Ereignissen im Ereignisprotokoll anzeigen

```
kesl-control -E --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

Informationen zu bestimmten Objekten im Backup anzeigen

```
kesl-control -B --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

Bestimmte Objekte aus dem Backup löschen

```
kesl-control -B --mass-remove --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator>
'<value>']"
```

Wobei gilt:

- `<field>` ist der Name des Datenbankfelds.
- `<comparison operator>` ist eine der folgenden Vergleichsoperationen:
  - > – Größer als.
  - < ist „kleiner als“

- `like` entspricht dem angegebenen Wert. Bei der Angabe eines Werts können Sie %-Masken verwenden: Der logische Ausdruck `"FileName like '%etc%'"` legt beispielsweise die Einschränkung „enthält den Text ‚etc' im Feld FileName" fest

  > Der Vergleichsoperator `like` funktioniert nur mit Feldern, die als Text in der Datenbank gespeichert werden. Der `like`-Operator funktioniert nicht mit Feldern für Datum, Uhrzeit, Zahlen und andere Datentypen, die sich von Text unterscheiden.

- == – Ist gleich.
- != – Ist ungleich.
- >= – Größer oder gleich.
- <= ist „kleiner oder gleich"

- `<value>` ist der Wert des Felds. 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 YYYY-MM-DD hh:mm:ss angeben. Der Datums- und Uhrzeitwert wird vom Benutzer angegeben und von der Anwendung in der Ortszeit des Benutzers angezeigt.

Beispielausgabe von Informationen zu Ereignissen, die den Text "etc" im Feld "FileName" enthalten

```
kesl-control -E --query "FileName like '%etc%'"
```

Beispielausgabe von Informationen zu Ereignissen vom Typ "ThreatDetected"

```
kesl-control -E --query "EventType == 'ThreatDetected'"
```

Beispielausgabe von Informationen zu Ereignissen vom Typ "ThreatDetected", die von Aufgaben des Typs "ODS" generiert wurden

```
kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"
```

Beispielausgabe von Informationen zu Ereignissen, die nach dem im UNIX-Zeitstempelsystem angegebenen Datum generiert wurden (Anzahl der Sekunden, die seit 00:00:00 (UTC), 1. Januar 1970 vergangen sind)

```
kesl-control -E --query "Date > '1583425000'"
```

Beispielausgabe 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'"
```

Beispielausgabe von Informationen zu Dateien im Backup mit der Signifikanzstufe "Hoch"

```
kesl-control -B --query "DangerLevel == 'High'"
```

Anwendungseinstellungen exportieren und importieren

In Kaspersky Endpoint Security können zur Fehlerbehebung, Überprüfung der Einstellungen oder zur einfacheren Konfiguration der Anwendung auf Benutzergeräten alle Anwendungseinstellungen exportiert und importiert werden.

Gewähren Sie nur vertrauenswürdigen Benutzern Zugriff auf die Konfigurationsdatei. Bevor Sie Einstellungen in das Programm importieren, überprüfen Sie die Pfade zu den Verzeichnissen, Konfigurationsdateien, ausführbaren Dateien und zur Quarantäne. Importieren Sie keine Konfigurationsdateien aus nicht vertrauenswürdigen Quellen. Eine Kompromittierung der Konfigurationsdatei kann die Sicherheit, Integrität oder Funktionsfähigkeit der Infrastruktur Ihres Unternehmens sowie die Benutzerdaten beeinträchtigen.

Einstellungen exportieren

Wenn Sie Einstellungen exportieren, werden alle Anwendungseinstellungen (einschließlich der allgemeinen Einstellungen der Untersuchung von Containern, der Einstellungen zur Untersuchung des Netzwerkverkehrs, der allgemeinen Anwendungseinstellungen und der Aufgabeneinstellungen) in der Konfigurationsdatei gespeichert. Sie können diese Konfigurationsdatei verwenden, um anschließend Einstellungen in das Programm zu importieren.

Programmeinstellungen exportieren

```
kesl-control --export-settings --file <configuration file path> [--json]
```

Wobei gilt:

- `--file <configuration file path>` ist der vollständige Pfad zur Konfigurationsdatei, in der Sie die App-Einstellungen speichern möchten.
- `--json` wird angegeben, um die Einstellungen in die Konfigurationsdatei im JSON-Format zu exportieren. Wenn Sie den Schalter `--json` nicht angeben, erfolgt der Export in eine Datei im INI-Format.

Importeinstellungen

1. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control --import-settings --file <configuration file path> [--json]
   ```

Wobei gilt:

- `--file <configuration file path>` ist der vollständige Pfad zur Konfigurationsdatei, aus der Sie Programmeinstellungen importieren möchten.
- `--json` wird angegeben, um die Einstellungen aus der Konfigurationsdatei im JSON-Format zu importieren. Wenn Sie den Schalter `--json` nicht angeben, versucht die Anwendung, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

2. Starten Sie das Programm neu.

Besonderheiten und Einschränkungen beim Exportieren und Importieren von Einstellungen

- Während des Imports und Exports von Einstellungen muss die Anwendung ausgeführt werden.
- Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, können die Einstellungen der vordefinierten Aufgabe des `Update` Typs nicht exportiert oder importiert werden.
- Wenn das Ändern der Einstellungen durch eine Richtlinie untersagt ist, ist der Import der Einstellungen nicht verfügbar.
- Wenn Sie Einstellungen, die aus einer älteren Programmversion exportiert wurden, in eine neuere Version importieren, werden die Einstellungen, die in der älteren Version nicht vorhanden waren, auf Standardwerte gesetzt.
- Sie können keine Einstellungen aus einer neueren Version in eine ältere Version importieren.
- Einige Richtlinien- und Aufgabeneinstellungen können aus den Versionen 12.3 und 12.4 des Web-Plug-ins des Programms nicht in die Version 12.5 des Programms importiert werden. Die Einschränkung gilt für die folgenden Richtlinien- und Aufgabeneinstellungen:
  - Schutzbereich und Ausnahmebereich für Schutz vor bedrohlichen Dateien und Schutz vor Verschlüsselung
  - Ausnahmen für Prozesse von der Untersuchung durch die Verhaltensanalyse
  - Vertrauenswürdige Geräte für die Gerätekontrolle
  - Untersuchungsbereich und Ausnahmebereich der Überwachung der Systemintegrität
  - Regeln für die Web-Kontrolle
  - Proxy-Server-Einstellungen
  - Ausnahme von der Untersuchung des Prozessspeichers
  - Globale Ausnahmen (von der Untersuchung ausgeschlossene Mount-Punkte)
  - Untersuchungsbereiche der Aufgaben *ODS, ContainerScan*, *InventoryScan* und *ODFIM*.
- Nach dem Import der Einstellungen wird Folgendes deaktiviert: Kaspersky Security Network (`UseKSN=No`), Cloud-Modus (`CloudMode=No`) und MDR-Integration (`UseMDR=No`). Konfigurieren Sie die Einstellungen, wenn Sie diese Funktion verwenden möchten.

- Durch dem Import der Anwendungseinstellungen können sich die internen Aufgaben-IDs ändern. Es wird empfohlen, zur Aufgabenverwaltung die Aufgabennamen zu verwenden.
- Bei der Integration mit Kaspersky Endpoint Detection and Response Expert (cloud) werden alle Einstellungen exportiert, einschließlich der Einstellungen, die von Kaspersky Endpoint Detection and Response Expert (cloud) empfangen wurden:
  - Adresse und Port des Servers für Telemetriedaten
  - Adresse und Port des Response-Servers
  - Verbindungstimeout für die Response-Server
  - Antworttimeout für den Response-Server
  - Verbindungstimeout für die Server für Telemetriedaten
  - Antworttimeout für den Server für Telemetriedaten
  - Client-Zertifikat des Servers für Telemetriedaten
  - Serverzertifikat des Servers für Telemetriedaten
  - Client-Zertifikat des Response-Servers
  - Serverzertifikat des Response-Servers

  Beim Import werden die oben aufgeführten Einstellungen nicht auf das Gerät importiert.

Verwaltung der Anwendung über die grafische Benutzeroberfläche

Für die Verwaltung des Programms über die grafische Benutzeroberfläche sind die Rechte der Rolle Administrator (admin) erforderlich.

Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, wird die grafische Benutzeroberfläche nicht unterstützt.

Im **Standard-Modus** des Programms können Sie die grafische Benutzeroberfläche verwenden, um folgende Aktionen auszuführen:

- Informationen zum Schutzstatus des Geräts anzeigen.
- Programmkomponenten konfigurieren.

  Auswahlstruktur

  - Schutz vor bedrohlichen Dateien.
  - Firewall-Verwaltung.

- Schutz vor Verschlüsselung.
- Untersuchung von Wechseldatenträgern.
- Schutz vor Web-Bedrohungen.
- Schutz vor E-Mail-Bedrohungen.
- Gerätekontrolle.
- Schutz vor Netzwerkbedrohungen.
- Schutz vor modifizierten USB-Geräten.
- Verhaltensanalyse.
- Exploit-Prävention.
- Programmkontrolle.
- Web-Kontrolle.
- Überwachung der Systemintegrität.

- Dateien und Verzeichnisse untersuchen, einschließlich des Sendens von Dateien an die Sandbox zur Untersuchung.
- Ein Update starten und Datenbanken-Updates rückgängig machen.
- Kaspersky Security Network für das Programm aktivieren oder deaktivieren.
- Beim Administrator des lokalen Netzwerks der Organisation temporären Zugriff auf ein blockiertes Gerät anfordern und erhalten.
- Lizenzschlüssel des Programms verwalten und Informationen zu aktuell verwendeten Lizenzen und Schlüsseln anzeigen.
- Informationen zu Objekten anzeigen, die im Backup abgelegt wurden.
- Programmberichte anzeigen.
- Protokolldateien der Anwendung erstellen.

App-Symbol im Infobereich

Über das Anwendungssymbol von Kaspersky Endpoint Security im Infobereich der Taskleiste das Kontextmenü und das Hauptfenster der grafischen Oberfläche der Anwendung aufgerufen werden.

Auf einigen Betriebssystemen fehlt nach der Installation des Pakets für die grafische Oberfläche der Anwendung möglicherweise das Anwendungssymbol standardmäßig.

Das Kontextmenü der Anwendung enthält die folgenden Punkte:

- **Kaspersky Endpoint Security 12.5 für Linux**. Öffnet das Hauptfenster der grafischen Benutzeroberfläche des Programms.
- **Beenden**. Beendet die grafische Benutzeroberfläche.

Hauptfenster der grafischen Oberfläche der Anwendung



Programmhauptfenster

Schutzstatus	Informationen zum Schutzstatus des Geräts. Wird im oberen Teil des Hauptfensters angezeigt. Sie können auf die Schaltfläche **Anzeigen** klicken, um das Fenster **Schutz-Center** zu öffnen. In diesem Fenster werden Empfehlungen zu Aktionen angezeigt, die ausgeführt werden müssen, um Schutzprobleme (falls vorhanden) zu beheben.
Untersuchung	Informationen zum Status der Aufgabe zur Schadsoftware-Untersuchung und zur Anzahl der gefundenen Bedrohungen. Sie können auf diesen Abschnitt klicken, um das Fenster **Untersuchung** zu öffnen. In diesem Fenster können Sie die Aufgaben *Schadsoftware-Untersuchung*, *Untersuchung wichtiger Bereiche* und *Untersuchung von Containern* starten und beenden sowie Berichte für diese Aufgaben anzeigen.
Update	Informationen zum Status der Aufgabe zum Datenbanken-Update. Sie können auf diesen Abschnitt klicken, um das Fenster **Update** zu öffnen. In diesem Fenster können Sie die Aufgaben *Update* und *Rollback* starten und Berichte für diese Aufgaben anzeigen.
Berichte	Anzeigen von Berichten und Statistiken für Komponenten und Aufgaben.
Backup	Anzeigen von Objektdetails im Backup. Vorgehensweise, wenn die Schaltfläche inaktiv ist
Einstellungen	Aktivieren oder Deaktivieren von Programmkomponenten, Konfigurieren von Kaspersky Security Network. Vorgehensweise, wenn die Schaltfläche inaktiv ist
Temporärer Zugriff	Anfordern und Erhalten von temporärem Zugriff auf ein gesperrtes Gerät.

Support	Informationen über das Programm: aktuelle Version von Kaspersky Endpoint Security, Datum der Veröffentlichung der Datenbank, Schlüssel und andere Informationen. Sie können auch die Kaspersky-Ressourcen besuchen, um nützliche Informationen zu erhalten, oder sich an den Technischen Support wenden.
Gültigkeitsdauer der Lizenz	Verbleibende Gültigkeitsdauer der Lizenz Sie können auf diesen Bereich klicken, um das Fenster **Lizenzen** zu öffnen. In diesem Fenster können Sie detaillierte Informationen zu Ihrer Lizenz anzeigen oder die Kaspersky-Website besuchen, um eine neue Lizenz zu erwerben.

Überwachung des Schutzstatus

Schutzstatus von Client-Geräten in Kaspersky Security Center

Mithilfe der Status von Client-Geräten können Sie in Kaspersky Security Center Informationen über den Schutzstatus eines Geräts abrufen. In Kaspersky Security Center gilt ein Gerät, auf dem der Kaspersky Security Center Administrationsagent installiert ist, als Client-Gerät.

Der Status des Client-Geräts kann gemäß den in Kaspersky Security Center konfigurierten Regeln in *Kritisch* oder *Warnung* geändert werden. Der Status kann sich beispielsweise ändern, wenn auf dem Gerät kein Schutzprogramm installiert ist, wenn seit längerer Zeit keine Untersuchung auf Viren durchgeführt wurde, wenn die Programmdatenbanken veraltet sind, wenn die Lizenz abgelaufen ist oder wenn Kaspersky Security Center den Gerätestatus von einem verwalteten Programm erhalten hat.

Weitere Informationen zu den Gründen für Statusänderungen und zum Konfigurieren der Bedingungen für die Zuweisung von Status finden Sie in der Hilfe zu Kaspersky Security Center.

Überprüfen des Schutzstatus eines Geräts in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Asset-Management** → **Assets (Geräte)** aus.

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Um eine verschachtelte Gruppe auszuwählen, klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Hierarchie anzeigen**.

   In der Liste werden nur die verwalteten Geräte der ausgewählten Administrationsgruppe angezeigt.

3. Klicken Sie auf den Namen eines Geräts.

4. Daraufhin wird das Eigenschaftenfenster des verwalteten Geräts geöffnet. Wählen Sie in diesem Fenster 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** gibt die Gesamtanzahl der bösartigen Objekte an, die seit der Installation von Kaspersky Endpoint Security auf dem ausgewählten Gerät gefunden wurden (Zähler für gefundene Bedrohungen).

- **Objekte, die nicht desinfiziert werden konnten** – Anzahl der infizierten Objekte, die von der Anwendung Kaspersky Endpoint Security nicht desinfiziert werden konnten.

Überprüfen des Schutzstatus eines Geräts in der Verwaltungskonsole

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 Anwendungen erkannt wurden, die auf dem Client-Gerät installiert sind. Jedes Problem hat einen Status, den Ihnen die Anwendung 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 Anwendung (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.

Weitere Informationen zu den Status von Client-Geräten finden Sie in der Hilfe zu Kaspersky Security Center.

Allgemeine Informationen zum Betrieb des Programms auf dem Gerät

Anzeigen allgemeiner Informationen über das Programm in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Asset-Management → Assets (Geräte)** aus.

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Um eine verschachtelte Gruppe auszuwählen, klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Hierarchie anzeigen**.

   In der Liste werden nur die verwalteten Geräte der ausgewählten Administrationsgruppe angezeigt.

3. Klicken Sie auf den Namen eines Geräts.

4. Wechseln Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts zur Registerkarte **Anwendungen**.

5. Klicken Sie in der Liste der auf dem Gerät installierten Anwendungen auf den Namen der Anwendung Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der App wird geöffnet.

6. Zeigen Sie die allgemeinen Informationen über das Programm auf der Registerkarte **Allgemein** im Abschnitt **Informationen** an:

   - **Name** – Name der Anwendung.
   - **Versionsnummer** – Versionsnummer der Anwendung.
   - **Installiert** – Datum und Uhrzeit der Installation der Anwendung auf dem Gerät.
   - **Letztes Software-Update**: Datum und Uhrzeit des letzten Updates der Softwaremodule von Kaspersky Endpoint Security.
   - **Letzte Synchronisierung** – Datum und Uhrzeit der letzten Verbindung des Geräts mit dem Administrationsserver von Kaspersky Security Center.
   - Der **Aktuelle Status** ist der Zustand des Programms auf dem Gerät, beispielsweise *Wird ausgeführt* oder *Angehalten*.
   - Der Block **Installierte Updates** enthält Informationen zu den installierten Versionen der Updates für die Anwendung.
   - Der Block **Anwendungsdatenbank** enthält für die Anwendungsdatenbank Informationen über Datum und Uhrzeit der Veröffentlichung des Updates sowie Datum und Uhrzeit der letzten Aktualisierung.

7. Zeigen Sie Informationen über die Funktionskomponenten des Programms auf der Registerkarte **Allgemein** im Abschnitt **Komponenten** an. Für jede Komponente wird ihr Status (z. B. *Gestoppt, Angehalten, Nicht installiert*) und ihre Version angezeigt.

8. Zeigen Sie die Liste der Programmereignisse auf dem Gerät auf der Registerkarte **Ereignisse** an.

Anzeigen allgemeiner Informationen über das Programm in der Verwaltungskonsole

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 Kaspersky-Anwendungen angezeigt.

5. Wählen Sie Kaspersky Endpoint Security aus und doppelklicken Sie darauf, um das Fenster mit den Programmeigenschaften zu öffnen. Alternativ können Sie die Schaltfläche **Eigenschaften** im unteren Bereich des Fensters verwenden.

   Das Eigenschaftenfenster der App wird geöffnet.

6. Zeigen Sie allgemeine Informationen über die Programmlinie im Abschnitt **Allgemein** an.

   - **Versionsnummer**: die Versionsnummer des Programms.
   - **Installiert** – Datum und Uhrzeit der Installation der Anwendung auf dem Gerät.
   - Der **Aktuelle Status** ist der Status des Programms (des kesl-Dienstes). Das Programm kann einen Status wie *Wird ausgeführt* oder *Angehalten* aufweisen.
   - **Letztes Software-Update**: Datum und Uhrzeit des letzten Updates der Softwaremodule von Kaspersky Endpoint Security.
   - **Installierte Updates** – Informationen zu installierten Versionen der Updates für die Anwendung.
   - **Anwendungsdatenbanken** – Datum und Uhrzeit der Veröffentlichung des Datenbanken-Updates der Anwendung.

7. Zeigen Sie Informationen über die Funktionskomponenten des Programms im Abschnitt **Komponenten** an. Für jede Komponente wird ihr Status (z. B. *Gestoppt, Angehalten, Nicht installiert*) und ihre Version angezeigt.

Anzeigen allgemeiner Informationen über das Programm in der Befehlszeile

Führen Sie den folgenden Befehl aus:

```
kesl-control --app-info [--json] [--check-permissions]
```

Wobei gilt:

`--json` – Gibt Daten im JSON-Format aus.

`--check-permissions` zeigt Pfade zu Programmverzeichnissen mit falsch konfigurierten Berechtigungen an.

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

- **Name**. Anwendungsname.
- **Version**. Aktuelle Version der App.
- **Richtlinie**. Informationen darüber, ob die Richtlinie von Kaspersky Security Center auf dem Gerät angewendet wird.
- Erweiterte Informationen zur Richtlinie, die auf dem Gerät angewendet wird:
  - Name der Richtlinie
  - Datum und Uhrzeit der letzten Anwendung oder Aktualisierung der Richtlinie auf dem Gerät.
  - Die Administrationsgruppe von Kaspersky Security Center, der das Gerät angehört.
  - Liste der Richtlinienprofile, die auf das Gerät angewendet werden (falls vorhanden).

Die erweiterten Informationen zu Richtlinien werden angezeigt, wenn für die Richtlinie von Kaspersky Endpoint Security in den Einstellungen des Administrationsagenten, der auf dem Gerät installiert ist, das Abrufen der erweiterten Richtliniendaten aktiviert ist (**Die Anwendung darf erweiterte Richtliniendaten des Geräts abrufen**). Der Parameter ist standardmäßig deaktiviert. Weitere Informationen zu den Einstellungen des Administrationsagenten finden Sie in der Hilfe zu Kaspersky Security Center.

- Informationen über die Lizenz, unter der das Programm verwendet wird:
  - **Informationen zur Lizenz der Anwendung**. Informationen über die Lizenz des Programms oder Status des Lizenzschlüssels des Programms.
  - **Ablaufdatum der Lizenz für Kaspersky Endpoint Security**. Datum und Uhrzeit des Ablaufs der Programmlizenz (UTC).
- Lizenzinformationen für die Komponente Endpoint Detection and Response Optimum und für Komponenten zur Integration mit Kaspersky-Lösungen. Die Felder werden angezeigt, wenn die folgenden Komponenten auf dem geschützten Gerät aktiviert sind:
  - **Informationen über die Lizenz von EDR Optimum**. Informationen über die Lizenz, unter der Kaspersky Endpoint Detection and Response Optimum aktiviert wurde, oder Status des Lizenzschlüssels von EDR Optimum.
  - **Ablaufdatum der Lizenz** für **EDR Optimum**. Datum und Uhrzeit (UTC) des Ablaufs der Gültigkeit der Lizenz.
  - **Informationen über die KUMA-Lizenz**. Informationen über die Lizenz, unter der die Funktionen der Kaspersky Unified Monitoring and Analysis Platform genutzt werden, oder über den Status des KUMA-Lizenzschlüssels.
  - **Gültigkeitsdauer der KUMA-Lizenz**. Datum und Uhrzeit (UTC) des Ablaufs der Gültigkeit der Lizenz.
  - **Informationen über die MDR-Lizenz**. Informationen über die Lizenz, unter der Kaspersky Managed Detection and Response Optimum aktiviert wurde, oder über den Status des MDR-Lizenzschlüssels.
  - **Gültigkeitsdauer der MDR-Lizenz**. Datum und Uhrzeit (UTC) des Ablaufs der Gültigkeit der Lizenz.
  - **Lizenzinformationen für EDR Expert (on-premise)**. Informationen über die Lizenz, mit der die Komponente Endpoint Detection and Response Expert (on-premise) aktiviert wurde, oder über den Status des Lizenzschlüssels für EDR Expert (on-premise).
  - **Ablaufdatum der Lizenz für EDR Expert (on-premises)**. Datum und Uhrzeit (UTC) des Ablaufs der Gültigkeit der Lizenz.
  - **Lizenzinformationen für EDR Expert (cloud)**. Informationen über die Lizenz, mit der die Komponente Endpoint Detection and Response Expert (on-premise) aktiviert wurde, oder über den Status des Lizenzschlüssels für EDR Expert (cloud).
  - **Ablaufdatum der Lizenz für EDR Expert (cloud)**. Datum und Uhrzeit (UTC) des Ablaufs der Gültigkeit der Lizenz.
- **Abonnementstatus**. Status des Abonnements. Dieses Feld wird angezeigt, wenn die App im Rahmen eines Abonnements ausgeführt wird.
- **Status der MDR-BLOB-Datei**. Der Status der MDR-BLOB-Datei, die zur Integration von Kaspersky Managed Detection and Response verwendet wird.

- **Ablaufdatum der Lizenz aus der MDR-BLOB-Datei**. Datum und Uhrzeit (UTC) des Ablaufs der Lizenz zur Nutzung der Funktionen von Kaspersky Managed Detection and Response. Dieses Feld wird angezeigt, wenn die BLOB-Konfigurationsdatei zur Integration mit Kaspersky Managed Detection and Response hochgeladen wurde.
- **Backup-Status**. Informationen zum Status des Backup-Speichers.
- **Backup-Verwendung**. Größe des Backups.
- **Letztes Ausführungsdatum der Aufgabe Scan_My_Computer**. Der Zeitpunkt, an dem die Aufgabe Schadsoftware-Untersuchung zuletzt ausgeführt wurde.
- **Veröffentlichungsdatum der verwendeten Programm-Datenbanken**. Uhrzeit der letzten Veröffentlichung der Anwendungsdatenbanken.
- **Programm-Datenbanken geladen**. Informationen darüber, ob die App-Datenbanken geladen sind.
- **Status des aktualisierbaren Kernel-Moduls**. Informationen zum Status des aktualisierbaren Kernel-Moduls.
- **Verwendung von Kaspersky Security Network**. Informationen zur Verwendung von Kaspersky Security Network: `Erweiterter KSN-Modus`, `Standardmäßiger KSN-Modus` oder `Deaktiviert`.
- **Light Agent-Modus**. Informationen über die Verwendung des Programms im Light Agent-Modus. Wenn das Programm im Standard-Modus oder im Endpoint Detection and Response Agent-Modus verwendet wird, wird diese Zeile nicht angezeigt.
- **Modus als Endpoint Detection and Response Agent**. Informationen über die Verwendung des Programms im EDR Agent-Modus. Wenn die Anwendung im Standard-Modus oder im Light Agent-Modus verwendet wird, wird diese Zeile nicht angezeigt.
- **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.
- **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 Systemintegrität**. 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 BadUSB-Angriffen**. Status der Komponente Schutz vor BadUSB-Angriffen.
- **Schutz vor Netzwerkbedrohungen**. Status der Komponente Schutz vor Netzwerkbedrohungen.
- **Verhaltensanalyse**. Status der Komponente Verhaltensanalyse.
- **Programmkontrolle**. Status der Komponente Programmkontrolle.
- **Web-Kontrolle**. Status der Komponente Web-Kontrolle.
- **Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)**. Status der Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA).
- **Integration mit Kaspersky Endpoint Detection and Response Expert (cloud)**. Status der Integration mit Kaspersky Endpoint Detection and Response Expert (cloud).
- **Integration mit Sandbox**. Status der Integration mit Sandbox.
- **Integration mit Kaspersky Unified Monitoring and Analysis Platform**. Status der Integration mit der Kaspersky Unified Monitoring and Analysis Platform.
- **Integration mit Kaspersky Network Detection and Response (KATA)** Status der Integration mit Kaspersky Network Detection and Response (KATA).
- **Schutz vor E-Mail-Bedrohungen**. Status der Komponente Schutz vor E-Mail-Bedrohungen.
- **Aktionen nach dem Update**. Verfügbarkeit von App-Updates und Aktionen, die der Benutzer ausführen muss.
- **Anwendung ist instabil**. Informationen zur Dump-Erstellung bei einem Programmabsturz. Dieses Feld wird angezeigt, wenn im Dump-Verzeichnis Dateien gefunden werden.
- **Programmstatus**. Informationen über den Verbindungsstatus des Administrationsagenten und die Berechtigungen für Systemverzeichnisse:
  - *OK*. Der Administrationsagent ist verbunden, die Berechtigungen für Systemverzeichnisse sind korrekt konfiguriert.
  - *Kritisch. Keine Verbindung zum Administrationsagenten*.
  - *Kritisch. Berechtigungen für Systemverzeichnisse sind fehlerhaft konfiguriert*.
  - *Kritisch. Keine Verbindung zum Administrationsagenten. Berechtigungen für Systemverzeichnisse sind fehlerhaft konfiguriert*.

So zeigen Sie allgemeine Informationen über das Programm in der grafischen Benutzeroberfläche an

1. Öffnen Sie das Hauptfenster der grafischen Benutzeroberfläche des Programms.
2. Klicken Sie im unteren Bereich des Hauptfensters auf die Schaltfläche **Support**.

   Das Fenster **Support** wird geöffnet.

3. Allgemeine Informationen über das Gerät und das installierte Programm anzeigen:

   - Version der Anwendung
   - **Lizenzschlüssel** – Aktiver Haupt-Lizenzschlüssel, welcher der Anwendung hinzugefügt wurde, oder Information über das Fehlen eines Schlüssels. Durch Klicken auf den Link in diesem Feld wird das Fenster **Lizenzen** geöffnet, in dem detaillierte Lizenzinformationen angezeigt werden.
   - **Schlüsselstatus** – Informationen über den Status des aktiven Haupt-Lizenzschlüssels oder über das Fehlen eines aktiven Schlüssels.
   - **Veröffentlichungsdatum der Datenbank** – Status und Veröffentlichungsdatum der Anwendungsdatenbanken.
   - **Betriebssystem** – Informationen über das Betriebssystem des Geräts.
   - **Durch Anwendung verwaltet** – Informationen darüber, ob das Gerät unter Verwaltung einer Richtlinie steht.

   Wenn die Option **Anwendung kann erweiterte Richtliniendaten auf dem Gerät empfangen** in der Richtlinie des Administrationsagenten aktiviert ist, werden im Fenster auch die folgenden Informationen über die Richtlinie angezeigt, die auf dem Gerät mit der installierten Anwendung angewendet wird.

   - **Name der Richtlinie** – der Name der Richtlinie, unter der das Gerät mit der installierten Anwendung ausgeführt wird.
   - **Richtlinie angewendet am** – Datum und Uhrzeit, der letzten Anwendung oder Aktualisierung der Richtlinie auf dem Gerät mit der installierten Anwendung.
   - **Administrationsgruppe** – Name der Administrationsgruppe, die das Gerät mit der installierten Anwendung umfasst, das unter einer Richtlinie ausgeführt wird.
   - **Aktive Richtlinienprofile** –Liste der auf dem Gerät angewendeten aktiven Richtlinienprofile (sofern vorhanden).

Programmstatistiken

Sie können Statistiken für die am häufigsten untersuchten Dateien und gestarteten Prozesse anzeigen.

Sie können in der Konfigurationsdatei kesl.ini im Abschnitt `[ScannerImpactStats]` konfigurieren, wie das Programm Statistiken berechnet und anzeigt.

So zeigen Sie Untersuchungsstatistiken in der Web Console an

1. Wählen Sie im Hauptfenster der Web Console **Asset-Management** → **Assets (Geräte)** aus.

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Um eine verschachtelte Gruppe auszuwählen, klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Hierarchie anzeigen**.

   In der Liste werden nur die verwalteten Geräte der ausgewählten Administrationsgruppe angezeigt.

3. Klicken Sie auf den Namen eines Geräts.

4. Wechseln Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts zur Registerkarte **Anwendungen**.

5. Klicken Sie in der Liste der auf dem Gerät installierten Anwendungen auf den Namen der Anwendung Kaspersky Endpoint Security.

6. Wählen Sie im nächsten Fenster mit den Anwendungseigenschaften auf der Registerkarte **Anwendungseinstellungen** den Abschnitt **Statistiken** → **Untersuchungsstatistiken** aus.

7. Zeigen Sie im Fenster **Untersuchungsstatistiken** die Programmstatistiken an:

   - Im Block **Am häufigsten untersuchte Dateien (Schutz vor bedrohlichen Dateien)** wird neben den Pfaden der Dateien, die von der Komponente Schutz vor bedrohlichen Dateien am häufigsten untersucht werden, auch die Häufigkeit angezeigt, mit der die Komponente auf diese Dateien zugreift. Die Dateien werden nach Anzahl der Zugriffe in absteigender Reihenfolge angezeigt.

   - Im Abschnitt **Am häufigsten gestartete Prozesse** werden die Pfade zu den Prozessen, deren Starts von Kaspersky Endpoint Security am häufigsten erkannt werden, und die Anzahl ihrer Starts angezeigt. Die Pfade zu den Prozessen werden der Reihe nach mit absteigender Anzahl der Starts angezeigt.

   Sie können im oberen Bereich jedes Bereichs auf die Schaltflächen **Exportieren** klicken, um die entsprechenden Statistiken in eine Textdatei zu exportieren.

So zeigen Sie Untersuchungsstatistiken in der Verwaltungskonsole 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 Kaspersky-Anwendungen angezeigt.

5. Wählen Sie Kaspersky Endpoint Security aus und doppelklicken Sie darauf, um das Fenster mit den Programmeigenschaften zu öffnen. Alternativ können Sie die Schaltfläche **Eigenschaften** im unteren Bereich des Fensters verwenden.

6. Wählen Sie im nächsten Fenster den Abschnitt **Statistik** → **Untersuchungsstatistiken** aus.

7. Zeigen Sie die Programmstatistiken an:

   - Im Block **Am häufigsten untersuchte Dateien (Schutz vor bedrohlichen Dateien)** wird neben den Pfaden der Dateien, die von der Komponente Schutz vor bedrohlichen Dateien am häufigsten untersucht werden, auch die Häufigkeit angezeigt, mit der die Komponente auf diese Dateien zugreift. Die Dateien werden nach Anzahl der Zugriffe in absteigender Reihenfolge angezeigt.

   - Im Abschnitt **Am häufigsten gestartete Prozesse** werden die Pfade zu den Prozessen, deren Starts von Kaspersky Endpoint Security am häufigsten erkannt werden, und die Anzahl ihrer Starts angezeigt. Die Pfade zu den Prozessen werden der Reihe nach mit absteigender Anzahl der Starts angezeigt.

   Sie können unterhalb jedes Bereichs auf die Schaltflächen **Exportieren** klicken, um die entsprechenden Statistiken in eine Textdatei zu exportieren.

So zeigen Sie Untersuchungsstatistiken über die Befehlszeile an

Führen Sie den folgenden Befehl aus:

```
kesl-control [-S] --get-statistic [--files] [--processes]
```

Wobei gilt:

- `--files` – Statistiken über Dateien, die von der Komponente Schutz vor bedrohlichen Dateien am häufigsten untersucht werden, und die Häufigkeit, mit der die Komponente auf diese Dateien zugreift.
- `--processes` – Statistiken über die Prozesse, deren Starts Kaspersky Endpoint Security am häufigsten erkennt, und die Anzahl dieser Starts.

  Das Ausschließen von Prozessen aus der Untersuchung durch die Verhaltensanalyse entfernt die Prozesse nicht aus den Statistiken, verbessert aber die Leistung von Kaspersky Endpoint Security.

Wenn Sie keinen Parameter angeben, gibt die Anwendung drei Listen aus: Statistik über die am häufigsten untersuchten Dateien, Statistik über die am häufigsten gestarteten Prozesse und eine Liste der auf dem Gerät erkannten Mountpunkte.

Unter CentOS 5.2, 5.4, 6.4 und 6.6 werden keine Statistiken über häufig untersuchte Dateien erfasst.

Gefundene Mountpunkte

Sie können die Liste der auf dem Gerät gefundenen Mountpunkte anzeigen. In der Liste werden Informationen darüber angezeigt, ob der Mountpunkt zu den Untersuchungsausnahmen hinzugefügt wurde.

So zeigen Sie die Liste mit Mountpunkten in der Web Console an

1. Wählen Sie im Hauptfenster der Web Console **Asset-Management** → **Assets (Geräte)** aus.

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Um eine verschachtelte Gruppe auszuwählen, klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Hierarchie anzeigen**.

   In der Liste werden nur die verwalteten Geräte der ausgewählten Administrationsgruppe angezeigt.

3. Klicken Sie auf den Namen eines Geräts.

4. Wechseln Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts zur Registerkarte **Anwendungen**.

5. Klicken Sie in der Liste der auf dem Gerät installierten Anwendungen auf den Namen der Anwendung Kaspersky Endpoint Security.

6. Wählen Sie im nächsten Fenster mit den Anwendungseigenschaften auf der Registerkarte **Anwendungseinstellungen** den Abschnitt **Statistiken** → **Mountpunkte** aus.

   Das Fenster **Mountpunkte** wird geöffnet.

7. Zeigen Sie in der Tabelle Informationen über Mountpunkte an:

   - **Pfad zum Mountpunkt** – Pfad zum erkannten Mountpunkt auf dem Gerät.
   - **Namensraum** – Informationen darüber, ob er Mountpunkt im Namensraum erkannt wurde.
   - **Ausgeschlossen** – Informationen darüber, ob der Mountpunkt zu den Untersuchungsausnahmen hinzugefügt wurde.

   Die Pfade zu den Mountpunkten sind wie folgt sortiert:

   - statische MP, System-MP, Service-MP und andere MP
   - gemountete Snap-Pakete und MP innerhalb deren Namensräume
   - Vom Docker-Containerverwaltungssystem erstellte Einhängepunkte

   Durch Klicken auf die Schaltfläche **Exportieren** im oberen Bereich des Fensters über der Liste können Sie die Liste der Mountpunkte in eine Textdatei exportieren. Die Datei enthält eine Liste der Pfade zu den Mountpunkten sowie die Tags **[Namensraum]** und **[Ausgeschlossen]**.

So zeigen Sie die Liste mit Mountpunkten in der Verwaltungskonsole 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 Kaspersky-Anwendungen angezeigt.
5. Wählen Sie Kaspersky Endpoint Security aus und doppelklicken Sie darauf, um das Fenster mit den Programmeigenschaften zu öffnen. Alternativ können Sie die Schaltfläche **Eigenschaften** im unteren Bereich des Fensters verwenden.
6. Dadurch wird das Fenster mit den Programmeigenschaften geöffnet. Wählen Sie in diesem Fenster den Abschnitt **Statistik → Mountpunkte** aus.
7. Zeigen Sie in der Tabelle **Liste der Mountpunkte** Informationen über Mountpunkte an:

   - **Pfad zum Mountpunkt** – Pfad zum erkannten Mountpunkt auf dem Gerät.
   - **Namensraum** – Informationen darüber, ob er Mountpunkt im Namensraum erkannt wurde.
   - **Ausgeschlossen** – Informationen darüber, ob der Mountpunkt zu den Untersuchungsausnahmen hinzugefügt wurde.

Die Pfade zu den Mountpunkten sind wie folgt sortiert:

- statische MP, System-MP, Service-MP und andere MP
- gemountete Snap-Pakete und MP innerhalb deren Namensräume
- Vom Docker-Containerverwaltungssystem erstellte Einhängepunkte

Mit der Schaltfläche **Exportieren**, die oberhalb der Liste befindet, können Sie die Liste der Mountpunkte in eine Datei im Textformat exportieren. Die Datei enthält eine Liste der Pfade zu den Mountpunkten sowie die Tags `[Namensraum]` und `[Ausgeschlossen]`.

So zeigen Sie die Liste mit Mountpunkten über die Befehlszeile an

Führen Sie den folgenden Befehl aus:

```
kesl-control [-S] --get-statistic --mountpoints
```

Die Ausgabe zeigt die folgenden Informationen an:

- `[excluded]` gibt an, ob der Mountpunkt zu den Untersuchungsausnahmen hinzugefügt wurde.
- `[namespace]` – Informationen darüber, ob er Mountpunkt im Namensraum erkannt wurde.
- Pfad zum erkannten Mountpunkt auf dem Gerät.

Die Pfade zu den Mountpunkten sind wie folgt sortiert:

- statische MP, System-MP, Service-MP und andere MP
- gemountete Snap-Pakete und MP innerhalb deren Namensräume
- Vom Docker-Containerverwaltungssystem erstellte Einhängepunkte

Liste der Funktionen und Technologien

Über die Befehlszeile können Sie die Liste der Programmfunktionen anzeigen, einschließlich Statusinformationen (verwendet oder nicht verwendet) und der Linux-Technologien, mit denen diese Programmfunktionen implementiert sind.

Liste der Funktionen und Technologien anzeigen

```
kesl-control --supported-tech-info
```

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

Abfangen von Dateivorgängen:

Status: In Verwendung oder Nicht in Verwendung

Technologien: fanotify, Kernel-Modul für den Schutz vor bedrohlichen Dateien, aktualisierbares Kernel-Modul.

Abfangen des Prozessstarts:

Status: In Verwendung oder Nicht in Verwendung

Technologien: eBPF, kprobe, netlink, undefined, aktualisierbares Kernel-Modul.

Untersuchung des Netzwerkverkehrs:

Status: In Verwendung oder Nicht in Verwendung

Technologien: eBPF, iptables, undefined.

iptables-Dienstprogramm:

Status: In Verwendung oder Nicht in Verwendung

Technologien: ipv6, undefined, timeout, Unterstützung für mehrere Labels in Regeln.

Netzwerkisolation:

Status: In Verwendung oder Nicht in Verwendung

Technologien: eBPF, iptables, undefined.

Exploit-Prävention:

Status: In Verwendung oder Nicht in Verwendung

Technologien: undefined, aktualisierbares Kernel-Modul.

Echtzeit-Schutzstatus

Der Status des Echtzeit-Computerschutzes bestimmt den Status der Komponente „Schutz vor bedrohlichen Dateien“. Der Schutz vor bedrohlichen Dateien bietet ein Mindestmaß an Sicherheit für den Computer. Die Komponente wird zusammen mit Kaspersky Endpoint Security gestartet und untersucht Dateien in Echtzeit.

Echtzeit-Schutzstatus

Status in Kaspersky Security Center	Status in der Befehlszeile	Description
Wird ausgeführt	Gestartet	Die Aufgabe „Schutz vor bedrohlichen Dateien“ wurde gestartet und wird ausgeführt.
Wird gestartet	Wird gestartet oder Fortsetzen	Versuchen Sie, die Aufgabe „Schutz vor bedrohlichen Dateien“ zu starten. Warten Sie, bis die Aufgabe gestartet wurde.
Beendet	Angehalten oder Wird angehalten	Die Aufgabe „Schutz vor bedrohlichen Dateien“ wurde manuell beendet. Führen Sie die Aufgabe in Kaspersky Security Center oder lokal auf dem Computer aus. Wenn das Programm im Light Agent-Modus installiert ist, erhält das Gerät diesen Status, wenn keine Verbindung mit der SVM besteht.
Angehalten	Pause oder Unterbrochen	Die Aufgabe „Schutz vor bedrohlichen Dateien“ wurde manuell angehalten. Führen Sie die Aufgabe in Kaspersky Security Center oder lokal auf dem Computer aus.
Nicht festgelegt		Das Programm ist im EDR-Agent-Modus installiert. Die Komponente „Schutz vor bedrohlichen Dateien“ wird im Inform-Modus ausgeführt.
Unbekannt		Unbekannter Fehler.

So ermitteln Sie den Status des Echtzeit-Computerschutzes

Sie können den Status des Echtzeit-Computerschutzes in einer Konsole von Kaspersky Security Center in der Liste der verwalteten Geräte oder lokal auf Ihrem Computer ermitteln.

So ermitteln Sie den Echtzeit-Computerschutz in der Web Console

Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.

Der aktuelle Schutzstatus wird in der Geräteliste in der Spalte **Status des Echtzeitschutzes** angezeigt. Wenn die Spalte **Status des Echtzeitschutzes** fehlt, verwalten Sie die Spalteneinstellungen (⚙).

So ermitteln Sie den Echtzeit-Computerschutz über die Befehlszeile

Führen Sie den folgenden Befehl aus:

```
kesl-control --get-task-state 1
```

Daraufhin zeigt Kaspersky Endpoint Security Informationen über die Ausführung des Schutzes vor bedrohlichen Dateien im folgenden Format an:

Name: File_Threat_Protection	
ID	: 1
Typ	: OAS
Status	: <protection status>

Was zu tun ist, wenn der Status des Echtzeit-Computerschutzes nicht Wird ausgeführt ist

1. Stellen Sie sicher, dass in den Richtlinieneigenschaften der Schutz vor bedrohlichen Dateien aktiviert ist.
2. Stellen Sie sicher, dass das Programm aktiviert ist.
3. Versuchen Sie, die Aufgabe „Schutz vor bedrohlichen Dateien" auszuführen:

   So führen Sie die Aufgabe „Schutz vor bedrohlichen Dateien" in der Web Console aus

   1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.

      Die Liste der verwalteten Geräte wird geöffnet.
   2. Wählen Sie in der Liste das erforderliche Gerät und klicken Sie auf dessen Namen.
   3. Wechseln Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts zur Registerkarte **Aufgaben**.

      Dadurch wird eine Liste aller Aufgaben auf dem Gerät geöffnet.
   4. Wählen Sie die Aufgabe **Schutz vor bedrohlichen Dateien** aus und klicken Sie auf die Schaltfläche **Ausführen**.

So führen Sie die Aufgabe „Schutz vor bedrohlichen Dateien“ über die Befehlszeile aus

```
Führen Sie den folgenden Befehl aus:
```

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

Ereignisse und Berichte

Während der Ausführung der Anwendung treten verschiedene *Ereignisse* auf. Diese können rein informativ sein oder wichtige Informationen enthalten. Die Anwendung kann beispielsweise mithilfe von Ereignissen über erfolgreiche Updates der Anwendungsdatenbanken benachrichtigen oder auf eine Funktionsstörung einer Komponente hinweisen, die behoben werden muss.

Mit Kaspersky Endpoint Security können Sie Informationen über Ereignisse, die während der Anwendungsausführung auftreten, in die folgenden Protokolle eintragen:

- Ereignisprotokoll der Anwendung. Standardmäßig speichert das Programm Ereignisinformationen in den Datenbankdateien des Ereignisprotokolls, die sich im Verzeichnis /var/opt/kaspersky/kesl/private/storage befinden. Sie können die Einstellungen des Ereignisprotokolls der Anwendung 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 Anwendung 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 Anwendung in kurzer Zeit viele Ereignisse desselben Typs generiert werden, wechselt die Anwendung 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. Weitere 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.

- Bei Verwendung der grafischen Benutzeroberfläche des Programms – in Popup-Benachrichtigungen, wenn Benachrichtigungen anzeigen in den Richtlinieneigenschaften oder in den allgemeinen Programmeinstellungen aktiviert ist

Auf Basis der Ereignisse, die während der Ausführung der Anwendung 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 Anwendung 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 Anwendungsdatenbanken erhalten. Ausführliche Informationen zur Arbeit mit Berichten von Kaspersky Security Center finden Sie in der Hilfe zu Kaspersky Security Center.

- Die grafische Benutzeroberfläche von Kaspersky Endpoint Security zeigt Berichte über das Programm, seine Komponenten und Aufgaben an.

Inhalte von Berichten und Ereignissen

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 Anwendungseinstellungen
- 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
- Namen der Programmkategorien
- Webadressen von Repositories
- Dateinamen, Pfade der Dateien und Hash-Summen ausführbarer Dateien von Anwendungen

Regeln zum Maskieren von Zeichen in Dateipfaden

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'` besteht aus zwei Zeichen (Backslash + dem Zeichen „a“).

`'\\'` ist ein Zeichen (Backslash) – `'\\\\'` sind zwei Zeichen (Backslash + Backslash).

Protokollierung von Ereignissen im Protokoll des Betriebssystems konfigurieren

Ereignisse, die während der Ausführung von Kaspersky Endpoint Security auftreten, können im Protokoll des Betriebssystems (syslog) aufgezeichnet werden. Sie können die Aufzeichnung von Ereignissen in diesem Protokoll über die Web Console, die Verwaltungskonsole oder die Befehlszeile aktivieren oder deaktivieren.

Standardmäßig ist die Protokollierung von Ereignissen im Protokoll des Betriebssystems deaktiviert.

Wenn Kaspersky Endpoint Security im Standard-Modus oder im EDR-Agent-Modus ausgeführt und durch eine Richtlinie in Kaspersky Security Center verwaltet wird, werden Informationen über das Hinzufügen und Entfernen von Lizenzschlüsseln sowie über den Ablauf der Lizenz standardmäßig im Protokoll des Betriebssystems aufgezeichnet. In den Richtlinieneigenschaften, unter denen die Anwendung ausgeführt wird, können Sie die Ereignisse auswählen, die in das Protokoll des Betriebssystems geschrieben werden.

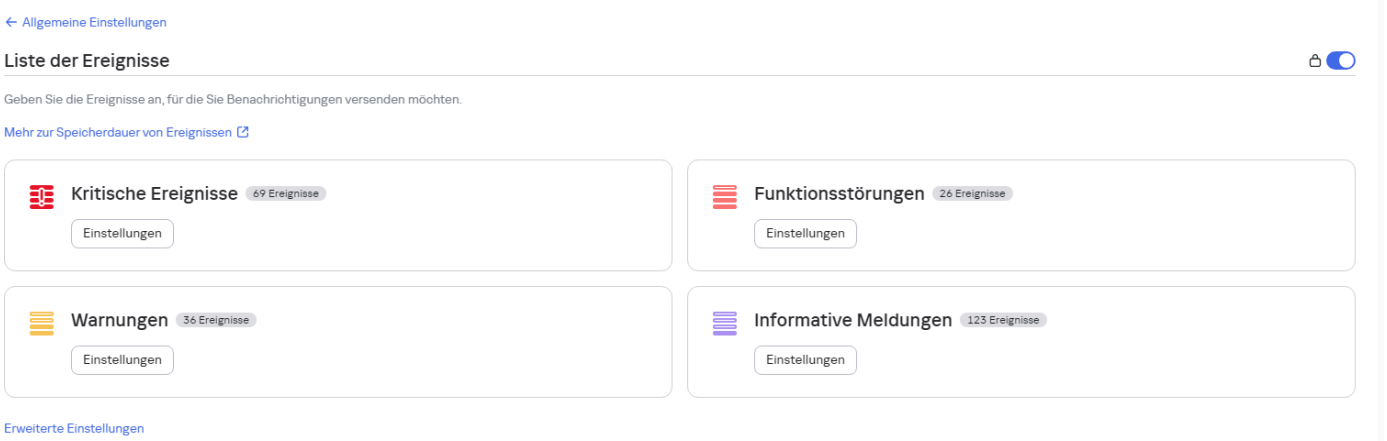
So konfigurieren Sie die Protokollierung von Ereignissen in syslog in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Asset-Management** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security für Linux.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Gehen Sie zur Registerkarte **Anwendungseinstellungen**.
4. Wählen Sie **Allgemeine Einstellungen** → **Ereigniseinstellungen** aus.

   Ereignistypen werden nach Schweregrad gruppiert angezeigt.
5. Klicken Sie im Block mit dem Namen des Schweregrads, der dem Ereignis entspricht, für das Sie die Protokollierung im Protokoll des Betriebssystems konfigurieren möchten, auf die Schaltfläche **Einstellungen**.

   Dadurch wird ein Fenster mit einer Liste aller Ereignisse des ausgewählten Schweregrads geöffnet. Sie können die Protokollierung im Protokoll des Betriebssystems für jedes Ereignis unabhängig aktivieren oder deaktivieren.
6. Klicken Sie in der Spalte **Ereignisse** auf den Namen des Ereignisses, für das Sie die Protokollierung im Protokoll des Betriebssystems konfigurieren möchten.
7. Gehen Sie zur Registerkarte **Benachrichtigungen**.
8. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Im Ereignisprotokoll des Betriebssystems speichern**.



Einstellungen für Ereignisbenachrichtigungen

So konfigurieren Sie die Protokollierung von Ereignissen in syslog 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.

4. Wechseln Sie zum Abschnitt **Allgemeine Einstellungen → Benutzeroberfläche**.

5. Klicken Sie unter **Benachrichtigungen** auf **Konfigurieren**.

   Das Fenster **Benachrichtigungseinstellungen** wird geöffnet.

6. Wählen Sie mithilfe der Kontrollkästchen die Ereignisse aus, die die App im Protokoll des Betriebssystems aufzeichnet.

   Sie können auch alle Ereignisse eines bestimmten Schweregrads auswählen:

   - *Kritische Ereignisse* sind Ereignisse, die eine ernsthafte Bedrohung für die Gerätesicherheit darstellen (Erkennung schädlicher Objekte, Schwachstellen, Probleme im Anwendungsbetrieb). Kritische Ereignisse erfordern Ihre sofortige Aufmerksamkeit. Es wird empfohlen, Benachrichtigungen für kritische Ereignisse aktiviert zu lassen.

   - *Fehler* sind Ereignisse, die auftreten, wenn eine Anwendung nicht ordnungsgemäß funktioniert (Funktionsfehler, Fehler in den Aufgabeneinstellungen). Diese Ereignisse stellen keine direkte Bedrohung für die Gerätesicherheit dar, erfordern aber Ihre Aufmerksamkeit, um den korrekten Anwendungsbetrieb zu gewährleisten.

   - *Warnungen* sind Ereignisse, die kein sofortiges Handeln erfordern, aber zukünftig eine Bedrohung für die Gerätesicherheit darstellen können.

   - *Info-Meldungen* sind Ereignisse mit informativem Charakter.

So konfigurieren Sie die Protokollierung von Ereignissen in syslog über die Befehlszeile

Über die Befehlszeile können Sie die Aufzeichnung von Ereignissen im Protokoll des Betriebssystems mithilfe des Parameters `UseSyslog` in den allgemeinen Anwendungseinstellungen aktivieren und deaktivieren.

Sie können den Wert des Parameters mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen enthält.

```
Aktivieren oder Deaktivieren des Protokollierens von Ereignissen im syslog

kesl-control --set-app-settings UseSyslog=<Yes|No>
```

Wobei gilt:

- `Yes`: Aktiviert das Speichern aller Ereignisse in syslog.
- `No` (Standardwert) – Protokollieren von Ereignissen im syslog deaktivieren.

Einstellungen des Ereignisprotokolls der Anwendung konfigurieren

Standardmäßig werden Informationen über Ereignisse im Ereignisprotokoll der Anwendung auf dem Gerät gespeichert.

Die Datenbank des Ereignisprotokolls enthält die folgenden Dateien:

- mehrere Dateien mit Ereignissen. Die Anzahl der Dateien hängt von der aktuellen Anzahl der Ereignisse im Ereignisprotokoll und der maximalen Anzahl der Ereignisse ab, die von der Anwendung gespeichert werden können (mittels Parameter `MaxEventsNumber`).

  Der Name der Ereignisdatei enthält die laufende Nummer der Erstellung (z. B. "events.db.0001"). Die Dateien werden erstellt, sobald sie voll sind. Wenn alle Ereignisdateien mit Ausnahme der ältesten Datei die Anzahl an Ereignissen erreichen, die dem angegebenen Parameterwert `MaxEventsNumber` entspricht, wird die älteste Datei gelöscht. Auf diese Weise kann die Anwendung mehr Ereignisse speichern als durch den Parameter angegeben.

- die Datenbank-Hauptdatei zur Verwaltung der Ereignisdateien, in denen die Informationen zu Dateien des Ereignisprotokolls gespeichert werden. Diese Datei kann nicht gelöscht werden.

Sie können die folgenden Optionen für das Ereignisprotokoll der App über die Befehlszeile mithilfe der allgemeinen App-Einstellungen verwalten:

- Ändern Sie mithilfe des Parameters `EventsStoragePath` den Pfad zur Datenbank-Hauptdatei des Ereignisprotokolls der Anwendung. Standardwert: /var/opt/kaspersky/kesl/private/storage/events.db
- Legen Sie mithilfe des Parameters `MaxEventsNumber` die maximale Anzahl von Ereignissen fest, welche die Anwendung speichern soll. Standardwert: 500000.

Sie können die aktuellen Einstellungen in den allgemeinen App-Einstellungen über die Befehlszeile oder in der Konfigurationsdatei anzeigen.

```
Aktuelle Werte der allgemeinen Einstellungen der App in der Konsole ausgeben

kesl-control --get-app-settings [--json]
```

Dabei wird `--json` angegeben, um die Einstellungen im JSON-Format auszugeben.

```
Aktuelle Werte der allgemeinen Einstellungen der App in eine Konfigurationsdatei ausgeben

kesl-control --get-app-settings --file <path to configuration file> [--json]
```

Dabei ist `--file <path to configuration file>` der Pfad zur Konfigurationsdatei, in die Sie die allgemeinen Einstellungen der App ausgeben möchten. 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.

Sie können die Werte der Einstellungen mithilfe von Befehlszeilenschaltern oder einer Konfigurationsdatei ändern, die alle allgemeinen Programmeinstellungen enthält.

```
Ereigniseinstellungen mithilfe von Befehlszeilenoptionen ändern

kesl-control --set-app-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Wobei <Name der Einstellung>=<Wert der Einstellung> der Name und der Wert einer der Einstellungen ist.

```
Ereigniseinstellungen mithilfe der Konfigurationsdatei ändern

kesl-control --set-app-settings --file <path to configuration file> [--json]
```

Wobei gilt:

- `--file <path to configuration file>` ist der vollständige Pfad zur Konfigurationsdatei mit den allgemeinen App-Einstellungen. Wenn Sie einen beliebigen Parameter in der Konfigurationsdatei löschen, wird nach Ausführung des Befehls der Standardwert für diesen Parameter zugewiesen.

- `--json` – Geben Sie diesen Schalter an, wenn Sie Einstellungen aus einer Konfigurationsdatei im JSON-Format importieren. Wenn die Option --json nicht angegeben ist, versucht die App, aus einer INI-Datei zu importieren. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Alle in der Datei angegebenen Werte der allgemeinen Einstellungen werden in die Anwendung importiert.

Programmereignisse anzeigen

Alle Ereignisse des Programms Kaspersky Endpoint Security in Kaspersky Security Center anzeigen

Ereignisse, die während des Betriebs von Kaspersky Endpoint Security auftreten, werden nach ihrer Wichtigkeit in folgende Typen unterteilt:

- *Kritische Ereignisse* sind Ereignisse, die eine ernsthafte Bedrohung für die Gerätesicherheit darstellen (Erkennung schädlicher Objekte, Schwachstellen, Probleme im Anwendungsbetrieb). Kritische Ereignisse erfordern Ihre sofortige Aufmerksamkeit. Es wird empfohlen, Benachrichtigungen für kritische Ereignisse aktiviert zu lassen.

- *Fehler* sind Ereignisse, die auftreten, wenn eine Anwendung nicht ordnungsgemäß funktioniert (Funktionsfehler, Fehler in den Aufgabeneinstellungen). Diese Ereignisse stellen keine direkte Bedrohung für die Gerätesicherheit dar, erfordern aber Ihre Aufmerksamkeit, um den korrekten Anwendungsbetrieb zu gewährleisten.

- *Warnungen* sind Ereignisse, die kein sofortiges Handeln erfordern, aber zukünftig eine Bedrohung für die Gerätesicherheit darstellen können.
- *Info-Meldungen* sind Ereignisse mit informativem Charakter.

Eine Liste aller Ereignisse während der Ausführung von Kaspersky Endpoint Security wird in der Web Console und in der Verwaltungskonsole angezeigt.

So zeigen Sie die Liste aller Ereignisse in der Web Console an

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wechseln Sie zur Registerkarte **Ereigniskonfiguration**.

   Es wird eine nach Schweregrad gefilterte Liste aller Ereignisse angezeigt.
4. Verwenden Sie das Menü auf der linken Seite, um alle Ereignisse anderer Schweregrade anzuzeigen.

So zeigen Sie die Liste aller Ereignisse in der Verwaltungskonsole an

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.
4. Wechseln Sie zum Abschnitt **Allgemeine Einstellungen** → **Benachrichtigungseinstellungen**.
5. Klicken Sie unter **Benachrichtigungen** auf **Konfigurieren**.

   Das Fenster **Benachrichtigungseinstellungen** wird geöffnet.

Sie können Benachrichtigungen über Ereignisse konfigurieren. 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 Anwendung oder das Versenden von Ereignisbenachrichtigungen per E-Mail konfigurieren. Ausführliche Informationen zur Verwendung von Benachrichtigungen in Kaspersky Security Center finden Sie in der Hilfe zu Kaspersky Security Center.

Ereignisse in der grafischen Oberfläche des Programms anzeigen

In der grafischen Benutzeroberfläche der Anwendung werden Informationen über Ereignisse standardmäßig in Pop-up-Benachrichtigungen angezeigt.

So konfigurieren Sie Popup-Benachrichtigungen in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Asset-Management** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security für Linux.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.

3. Gehen Sie zur Registerkarte **Anwendungseinstellungen**.

4. Wählen Sie **Allgemeine Einstellungen → Ereigniseinstellungen** aus.

5. Klicken Sie auf den Link **Zusätzliche Einstellungen**.

   Das Fenster **Zusätzliche Einstellungen** wird geöffnet.

6. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Popup-Benachrichtigungen in der grafischen Benutzeroberfläche anzeigen**. Dieses Kontrollkästchen ist standardmäßig aktiviert.

7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie Popup-Benachrichtigungen 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.

4. Wechseln Sie zum Abschnitt **Allgemeine Einstellungen → Benachrichtigungseinstellungen**.

5. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Popup-Benachrichtigungen in der grafischen Benutzeroberfläche anzeigen**. Dieses Kontrollkästchen ist standardmäßig aktiviert.

So konfigurieren Sie Popup-Benachrichtigungen über die Befehlszeile

Über die Befehlszeile können Sie das Anzeigen von Pop-up-Benachrichtigungen in der grafischen Benutzeroberfläche aktivieren oder deaktivieren, indem Sie den Parameter `ShowPopUpNotifications` aus den allgemeinen Anwendungseinstellungen verwenden.

Sie können den Wert der Einstellung mithilfe von Befehlszeilenschaltern oder einer Konfigurationsdatei ändern, die alle allgemeinen Programmeinstellungen enthält.

```
Aktiviert die Anzeige von Popup-Benachrichtigungen in der grafischen Benutzeroberfläche

kesl-control --set-app-settings ShowPopUpNotifications=<Yes|No>
```

Wobei gilt:

- `Yes` (Standardwert) – In der grafischen Benutzeroberfläche werden Pop-up-Benachrichtigungen angezeigt.
- `No` – In der grafischen Benutzeroberfläche werden keine Pop-up-Benachrichtigungen angezeigt.

Aktuelle Ereignisse des Programms Kaspersky Endpoint Security über die Befehlszeile anzeigen

Über die Befehlszeile können Sie Informationen zu allen aktuellen Ereignissen im Programm oder zu Ereignissen ausgeben, die mit der angegebenen Aufgabe zusammenhängen. Über einen Filter können Sie sich auch bestimmte aktuelle Ereignisse anzeigen lassen, beispielsweise Ereignisse eines bestimmten Typs.

```
Informationen zu allen aktuellen Programmereignissen in der Konsole anzeigen

kesl-control -W
```

Der Befehl gibt den Namen des Ereignisses und zusätzliche Informationen über das Ereignis zurück.

```
Die Aufgabe ausführen und Informationen zu aktuellen Ereignissen, die mit ihr verbunden sind, in der Konsole ausgeben

kesl-control --start-task <task ID|name> -W
```

Dabei ist `<task ID|name>` die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Der Befehl startet die Aufgabe mit der angegebenen ID oder dem angegebenen Namen und aktiviert die Ausgabe aktueller Ereignisse, die mit der Aufgabe verbunden sind. Ereignisse werden ausgegeben, sobald sie von dieser Aufgabe generiert werden.

```
Beispiel für das Starten der Aufgabe mit ID=1 und das Aktivieren der Ausgabe ihrer Ereignisse

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

```
Informationen zu aktuellen Ereignissen, die den Filterbedingungen entsprechen, in der Konsole anzeigen

kesl-control -W --query "<filter conditions>"
```

wobei `<filter conditions>` für einen oder mehrere logische Ausdrücke im Format `<field> <comparison operation> '<value>'` steht, die durch den logischen Operator `and` verbunden sind.

```
Beispiel für die Ausgabe des Ereignisses TaskStateChanged

kesl-control -W --query "EventType == 'TaskStateChanged'"
```

```
Beispiel für die Ausgabe des Ereignisses TaskSettingsChanged, ausgelöst durch den Benutzer 'User'

kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'"
```

Ereignisse aus dem Ereignisprotokoll des Programms ausgeben

Sie können über die Befehlszeile Informationen zu Ereignissen aus dem Ereignisprotokoll des Programms in die Konsole oder in eine Datei ausgeben. Um eine Teilmenge von Ereignissen auszugeben, verwenden Sie Filterung.

```
Informationen zu allen Ereignissen im Ereignisprotokoll der App in die Konsole ausgeben

kesl-control -E --query [--db <database file>]
```

wobei `<database file>` der vollständige Pfad zur Datenbankdatei des Ereignisprotokolls ist, aus der Ereignisse ausgegeben werden sollen.

Standardmäßig speichert das Programm Informationen zu Ereignissen in der Datenbank `/var/opt/kaspersky/kesl/private/storage/events.db`. Der Speicherort der Datenbank wird durch die allgemeine Programmeinstellung `EventsStoragePath` bestimmt.

Wenn sich das Ereignisprotokoll in der Standarddatenbank befindet, verwenden Sie den folgenden Befehl, um Ereignisse in die Konsole auszugeben:

```
kesl-control -E
```

Mit dem Tool `less` können Sie durch die Liste der angezeigten Ereignisse navigieren. Standardmäßig speichert die Anwendung bis zu 500.000 Ereignisse. Die maximale Anzahl von Ereignissen, die das Programm speichert, wird durch die allgemeine Programmeinstellung `MaxEventsNumber` festgelegt.

```
Informationen zu Ereignissen im Ereignisprotokoll des Programms, die bestimmten Kriterien entsprechen, in der Konsole anzeigen
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] [--json] [--reverse]
```

wobei:

- `<filter conditions>` gibt einen oder mehrere logische Ausdrücke im Format `<field> <comparison operator> '<value>'` an, die mit dem logischen Operator `and` kombiniert werden, um die Ergebnisse der Abfrage einzuschränken.
- `<number>` ist die Anzahl der neuesten Ereignisse in der Auswahl (d. h. die Anzahl der Datensätze, gezählt ab dem Ende der Auswahl), die Sie ausgeben möchten.
- `--json` – Gibt die Ereignisse im JSON-Format aus.
- `--reverse` – Ereignisse in umgekehrter Reihenfolge anzeigen (das neueste Ereignis steht oben und das ältesten unten).

```
Informationen zu allen Ereignissen im Ereignisprotokoll der App in eine Datei ausgeben
kesl-control -E --query "<>" [--db <database file>] [-n <number>] --file <path to file> [--json]
```

wobei `--file <path to file>` der vollständige Pfad zu der Datei ist, in die Ereignisse ausgegeben werden sollen.

Nützliche Artikel

Vorgehen bei Fehlalarmen

Berichte anzeigen

Das Anzeigen von Berichten ist nur in der grafischen Benutzeroberfläche des Programms verfügbar.

Informationen über die Ausführung der einzelnen Komponenten von Kaspersky Endpoint Security, die Ausführung der einzelnen Untersuchungsaufgaben, der Update-Aufgabe und der Aufgabe zur Integritätsprüfung sowie über die allgemeine Programmausführung werden in *Berichten* protokolliert.

Die Berichte enthalten folgende Ereigniskategorien:

- *Kritisch* – Das sind Ereignisse von kritischer Bedeutung, die Sie beachten müssen, da sie auf Probleme mit der Anwendung oder auf Schwachstellen beim Schutz Ihres Geräts hinweisen.
- *Hoch.*
- *Mittel.*
- *Niedrig.*
- *Informativ.*
- *Fehler.*

Die folgenden Berichte sind in der Anwendung verfügbar:

- **Statistik**. Statistische Daten zur Komponente „Schutz vor bedrohlichen Dateien“ und zu Untersuchungsaufgaben. Durch Klicken auf **Aktualisieren** können Sie den angezeigten Bericht aktualisieren.
- **Systemaudit**. Informationen über Ereignisse, die während der Programmausführung und während der Interaktion des Benutzers mit dem Programm auftreten.
- **Schutz vor Bedrohungen**. Informationen über Ereignisse, die während der Ausführung der folgenden Programmkomponenten protokolliert werden:
  - Komponente "Schutz vor bedrohlichen Dateien".
  - Untersuchung von Wechseldatenträgern
  - Schutz vor Verschlüsselung
  - Schutz vor Web-Bedrohungen
  - Schutz vor E-Mail-Bedrohungen
  - Schutz vor Netzwerkbedrohungen
  - Schutz vor modifizierten USB-Geräten
  - Firewall-Verwaltung
  - Programmkontrolle
  - Gerätekontrolle
  - Verhaltensanalyse
  - Exploit-Prävention

- Überwachung der System-Integrität
- Web-Kontrolle

- **Aufgaben auf Befehl**. Dieser Bericht enthält Informationen zu Ereignissen, die während der Ausführung von Untersuchungsaufgaben, Update-Aufgaben und Aufgaben zur Prüfung der Systemintegrität protokolliert werden.

- **Ausführungsprävention** Dieser Bericht enthält Informationen über Ereignisse, die während der Verhinderung der Objektausführung durch die Komponenten EDR Expert (on-premise) und EDR Optimum protokolliert wurden.

So zeigen Sie einen Bericht in der Programmoberfläche an

1. Öffnen Sie das Hauptfenster der grafischen Benutzeroberfläche des Programms.
2. Klicken Sie im unteren Bereich des Hauptfensters der Anwendung auf die Schaltfläche **Berichte**.

   Das Fenster **Berichte** wird geöffnet.
3. Wählen Sie im linken Bereich des Fensters **Berichte** den gewünschten Berichtstyp aus.

   Der Bericht wird im rechten Teil des Fensters angezeigt. 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.

   Standardmäßig werden die Ereignisse in aufsteigender Reihenfolge nach den Werten in der Spalte **Datum und Uhrzeit** sortiert. Zur Vereinfachung der Arbeit mit Berichten können Sie die Darstellung der Daten auf dem Bildschirm wie folgt ändern:

   - Filtern Sie die Liste der Ereignisse nach dem Zeitpunkt ihres Auftretens.
   - Suchen Sie mithilfe der Suchfunktion nach einem bestimmten Ereignis.
4. Ausführliche Informationen über ein bestimmtes Ereignis finden Sie im Bericht dieses Ereignisses.

   Am unteren Rand des Fensters wird ein Block angezeigt, der die Attribute dieses Ereignisses enthält.

Kennzahlen zum Systemzustand sammeln

Das Ausführen der Anwendung "Kaspersky Endpoint Security" hat Auswirkung auf das Betriebssystem. Um zu diese Auswirkungen zu analysieren, können Kennzahlen zur Leistung der Anwendung gesammelt werden.

Sie können Metriken in Datenvisualisierungstools wie Grafana analysieren. Die exportierten Kennzahlen können in komplexeren Monitoringsystemen wie Prometheus und Zabbix veröffentlicht werden.

```
Erfassung von Metriken für von der App verwendete Betriebssystemressourcen konfigurieren

kesl-control [-J] --export-metrics [--period <interval in seconds between outputs>|--interactive]
```

Wobei gilt:

`--period` aktiviert die regelmäßige Ausgabe der Ergebnisse in der Befehlszeile (mit dem in Sekunden angegebenen Ausgabeintervall).

`--interactive` – interaktive Ausgabe (durch Drücken der **`Eingabetaste`**)

Als Ergebnis der Ausführung des Befehls wird eine Liste mit Metriken ausgegeben:

Liste der Kennzahlen

Interne Bezeichnung der Metrik, Tag und Typ der Metrik	Beschreibung und empfohlener Schwellenwert
lfs_system_descriptor_opened_count Gauge	Die Anzahl der Handles, die der Prozess "kesl" aktuell geöffnet hat. Wenn die Anzahl der Deskriptoren um mehr als 250 pro Stunde zunimmt, empfehlen wir, sich an den Technischen Support zu wenden.
lfs_system_uptime_milliseconds Counter	Die Anzahl der Millisekunden, die seit dem Start des Betriebssystems bis zum aktuellen Zeitpunkt vergangen sind.
lfs_system_memory_usage_bytes Bezeichnung type=virtual Gauge	Die Menge des virtuellen Speichers, die aktuell vom Prozess "kesl" verwendet wird. Es wird empfohlen, den Schwellenwert anhand der Systemdaten eigenständig festzulegen. Sie können die Daten selbst abrufen oder ein Skript zur Erfassung notwendiger Informationen verwenden. Ein Beispielskript können Sie beim Technischen Support anfordern.
lfs_system_memory_usage_bytes Bezeichnung type=resident Gauge	Die Menge des residenten Speichers, die aktuell vom Prozess "kesl" verwendet wird. Es wird empfohlen, den Schwellenwert anhand der Systemdaten eigenständig festzulegen. Sie können die Daten selbst abrufen oder ein Skript zur Erfassung notwendiger Informationen verwenden. Ein Beispielskript können Sie beim Technischen Support anfordern.
lfs_system_memory_usage_bytes Bezeichnung type=swap Gauge	Die Menge an Auslagerungsspeicher, die derzeit vom kesl-Prozess verwendet wird. Es wird empfohlen, den Schwellenwert anhand der Systemdaten eigenständig festzulegen. Sie können die Daten selbst abrufen oder ein Skript zur Erfassung notwendiger Informationen verwenden. Ein Beispielskript können Sie beim Technischen Support anfordern.
lfs_system_memory_wd_limits_bytes Bezeichnung type=virtual Gauge	Beschränkung für die Verwendung des virtuellen Speichers des Prozesses "kesl".
lfs_system_memory_wd_limits_bytes Bezeichnung type=resident Gauge	Beschränkung der Verwendung des residenten Speichers des Prozesses "kesl".
lfs_system_memory_wd_limits_bytes Bezeichnung type=swap Gauge	Beschränkung der Verwendung des Auslagerungsspeichers durch den kesl-Prozess.
lfs_system_cpu_usage_milliseconds Bezeichnung type=user Counter	Die Anzahl der in Millisekunden gemessenen CPU-Zeit, die der Prozess "kesl" seit seinem Start im User Space bis zum aktuellen Zeitpunkt verbraucht hat. Es wird empfohlen, den Schwellenwert anhand der Systemdaten eigenständig festzulegen. Sie können die Daten selbst abrufen oder ein Skript zur Erfassung notwendiger Informationen verwenden. Ein Beispielskript können Sie beim Technischen Support anfordern.
lfs_system_cpu_usage_milliseconds Bezeichnung type=kernel Counter	Die Anzahl der in Millisekunden gemessenen CPU-Zeit, die der Prozess "kesl" seit seinem Start im Kernel Space bis zum aktuellen Zeitpunkt verbraucht hat. Es wird empfohlen, den Schwellenwert anhand der Systemdaten eigenständig festzulegen. Sie können die Daten selbst abrufen oder ein Skript zur Erfassung notwendiger Informationen verwenden. Ein Beispielskript können Sie beim Technischen Support anfordern.
lfs_system_cpu_usage_milliseconds Bezeichnung type=total Counter	Die Anzahl der in Millisekunden gemessenen CPU-Zeit, die der Prozess "kesl" seit seinem Start im User Space und im Kernel Space bis zum aktuellen Zeitpunkt verbraucht hat. Wenn die CPU-Zeit des Prozesses "kesl" die gesamte restliche Last übersteigt, wird es empfohlen, sich an den Technischen Support zu wenden.

Interne Bezeichnung der Metrik, Tag und Typ der Metrik	Beschreibung und empfohlener Schwellenwert
lfs_tcpSynInterceptor_connection_hanging_count Counter	Die Gesamtzahl der während der TCP-Verbindungsphase zwischen Server und Client angehaltenen Netzwerkverbindungen, vom Start des Prozesses "kesl" bis zum aktuellen Zeitpunkt (als angehalten gelten Verbindungen, die je nach Systemparameter "/proc/sys/net/ipv4/tcp_syn_retries" zwischen 1 Sekunde und 2 Minuten auf eine Entscheidung des Remote-Servers warten, ob die Verbindung zugelassen wird). Ein Anstieg kann darauf zurückzuführen sein, dass der Remote-Server nicht verfügbar ist oder fehlt. Wenn die Anzahl der angehaltenen Netzwerkverbindungen auf über 10 pro Minute ansteigt, wird es empfohlen, sich an den Technischen Support zu wenden.
lfs_tcpSynInterceptor_connection_count Gauge	Die Anzahl der Netzwerkverbindungen, die aktuell eine Verbindung mit dem Remote-Server abwarten.
lfs_tcpSynInterceptor_verdict_count Bezeichnung verdict=allow Counter	Gesamtzahl der abgefangenen Verbindungen, die erfolgreich hergestellt wurden, seit dem Start des Prozesses "kesl" bis zum aktuellen Zeitpunkt.
lfs_tcpSynInterceptor_verdict_count Bezeichnung verdict=drop Counter	Gesamtzahl der abgefangenen Verbindungen, für die keine erfolgreiche Verbindung hergestellt wurde, seit dem Start des Prozesses "kesl" bis zum aktuellen Zeitpunkt.
lfs_tcpSynInterceptor_verdict_count Bezeichnung verdict=unknown Counter	Gesamtzahl der Netzwerkverbindungen vom Start des kesl-Prozesses bis zum aktuellen Zeitpunkt, für welche die Entscheidung des Remote-Servers, ob die Verbindung zugelassen wird, aussteht.
lfs_tcpSynInterceptor_verdict_latency_milliseconds Histogram	Histogramm der Zeit, die ein Remote-Server benötigt, um eine Entscheidung über die Zulassung einer Verbindung zu treffen, vom Moment des Abfangens eines SYN-Pakets bis zur Entscheidung darüber.
lfs_tproxy_connection_count Bezeichnung direction=inbound Gauge	Die aktuelle Anzahl der eingehenden, abgefangenen Netzwerkverbindungen in diesem Moment.
lfs_tproxy_connection_count Bezeichnung direction=outbound Gauge	Die aktuelle Anzahl der ausgehenden, abgefangenen Netzwerkverbindungen in diesem Moment.
lfs_tproxy_connection_processed_count Bezeichnung direction=inbound Counter	Gesamtzahl der abgefangenen eingehenden Netzwerkverbindungen.
lfs_tproxy_connection_processed_count Bezeichnung direction=outbound Counter	Gesamtzahl der abgefangenen ausgehenden Netzwerkverbindungen.
lfs_tproxy_connection_orphaned_count Counter	Die Gesamtzahl der Verbindungen (seit dem Start der Komponenten "Schutz vor Web-Bedrohungen", "Schutz vor Netzwerkbedrohungen" und "Programmkontrolle"), die von Kaspersky Endpoint Security abgefangen wurden, obwohl dies nicht beabsichtigt war (z. B. aufgrund einer inkompatiblen iptables-Konfiguration oder weil die Anwendung die neue Abfangkonfiguration noch nicht verarbeiten konnte). Solche Verbindungen werden abgelehnt. Wenn die Gesamtzahl solcher Verbindungen 10 überschreitet, kann dies darauf hinweisen, dass die Anwendung oder das System nicht ordnungsgemäß funktionieren. Es wird empfohlen, den Technischen Support zu kontaktieren.
lfs_tproxy_threadPool_task_count Counter	Die Gesamtzahl der Aufgaben (neue Verbindung, neuer Datenteil, gesendete Daten usw.), die im Thread-Pool aufgenommen wurden, seit die Komponenten "Schutz vor Web-Bedrohungen", "Schutz vor Netzwerkbedrohungen" und "Web-Kontrolle" ausgeführt werden. Wenn der Unterschied zwischen der allgemeinen Anzahl an Aufgaben und der Anzahl an ausgeführten Aufgaben stetig ansteigt, müssen Sie weitere Ressourcen hinzufügen, Ausnahmen einrichten oder den Technischen Support kontaktieren.

Interne Bezeichnung der Metrik, Tag und Typ der Metrik	Beschreibung und empfohlener Schwellenwert
lfs_tproxy_threadPool_thread_count Gauge	Anzahl der Threads, die den MITM-Mechanismus des Netzwerk-Interceptors bedienen. Threads werden vom Thread-Manager erstellt, um Verbindungen zu verarbeiten. Alle Threads führen denselben Code aus, in dem sie auf Netzwerkereignisse warten, z. B. auf neue Verbindungen und eingehende Pakete über bestehende Verbindungen.
lfs_tproxy_threadPool_thread_waiting Gauge	Anzahl der freien Threads von lfs_tproxy_threadPool_thread_count. Threads, die im MITM-Mechanismus des Netzwerk-Interceptors auf Ereignisse warten.
lfs_tproxy_threadPool_task_duration_milliseconds Histogram	Histogramm der Ausführungszeit für Aufgaben, die abgefangene Verbindungen verarbeiten. Wenn die Ausführung von 95% der Aufgaben länger als 1 Sekunde dauert, müssen Sie weitere Ressourcen hinzufügen, Ausnahmen einrichten oder sich an den Technischen Support wenden.
lfs_tproxy_socket_count Gauge	Aktuelle Anzahl der Sockets (Listening-Sockets und Connecting-Sockets). Die abgefangene Verbindung verfügt über 2 Verbindungssockets.
lfs_trafficScanning_object_hanging_count Gauge	Die aktuelle Anzahl der angehaltenen Objektprüfungen im abgefangenen Datenverkehr (als angehaltene Prüfungen gelten jene, die länger als 1 Minute dauern). Wenn die Gesamtzahl hängender Objektuntersuchungen 35 überschreitet, weist dies auf ein Problem mit den Programmdatenbanken hin. In solchen Fällen empfehlen wir, den Technischen Support zu kontaktieren.
lfs_trafficScanning_object_duration_milliseconds Histogram	Histogramm der Zeit für die Objektprüfung im abgefangenen Datenverkehr. Wenn die Prüfung von 95% der Objekte länger als 1 Sekunde dauert, müssen Sie weitere Ressourcen hinzufügen, die Datenbanken aktualisieren oder sich an den Technischen Support wenden. Wenn die Wachstumsrate der Paketprüfungen im abgefangenen Datenverkehr 0 beträgt, aber die Kennzahl für "lfs_tproxy_threadPool_task_count" nicht 0 ist, müssen Sie die Anwendungsdatenbanken aktualisieren oder sich an den Technischen Support wenden.
lfs_fileMonitor_cache_size Gauge	Die aktuelle Größe des Caches für den File Monitor (Dateirevisions-Cache), der Dateiänderungen verfolgt. Wenn die aktuelle Größe des Caches für den File Monitor größer als 50.000 ist, wird es empfohlen, sich an den Technischen Support zu wenden.
lfs_fileMonitor_cache_hit_count Counter	Die Anzahl der Treffer im Cache von File Monitor (Dateirevisions-Cache), der Dateiänderungen verfolgt.
lfs_fileMonitor_cache_miss_count Counter	Die Anzahl der Cache-Fehler von File Monitor (Dateirevisions-Cache), der Dateiänderungen verfolgt.
lfs_faCache_file_count Gauge	Die aktuelle Cache-Größe der Dateien des fanotify-Interceptors, die keine Prüfung benötigen. Wenn die aktuelle Größe des Dateicaches 100000 übersteigt, wird es empfohlen, den technischen Support zu kontaktieren.
lfs_faCache_file_hit_count Counter	Die Anzahl der Cache-Treffer für die Dateien des fanotify-Interceptors, die keine Prüfung erfordern.
lfs_faCache_file_miss_count Counter	Die Anzahl der Cache-Fehler für die Dateien des fanotify-Interceptors, die keine Prüfung erfordern.
lfs_faCache_volume_count Gauge	Aktuelle Größe des Caches der Mountpunkte des fanotify-Interceptors.
lfs_oas_cache_file_count Gauge	Die aktuelle Cache-Größe der Dateien des Schutzes vor bedrohlichen Dateien, die nicht untersucht werden müssen. Wenn die aktuelle Größe des Dateicaches 100000 übersteigt, wird es empfohlen, den technischen Support zu kontaktieren.
lfs_oas_cache_file_hit_count Counter	Die Anzahl der Treffer im Cache der Dateien des Schutzes vor bedrohlichen Dateien, die nicht untersucht werden müssen.

Interne Bezeichnung der Metrik, Tag und Typ der Metrik	Beschreibung und empfohlener Schwellenwert
lfs_oas_cache_file_miss_count Counter	Die Anzahl Cache-Fehler für die Dateien des Schutzes vor bedrohlichen Dateien, die nicht untersucht werden müssen.
lfs_oas_cache_volume_count Gauge	Die aktuelle Größe des Caches der Mountpunkte für den Schutz vor bedrohlichen Dateien.
lfs_processManager_cache_size Gauge	Die aktuelle Anzahl aktiver Prozesse im System, die sich im Cache befinden.
lfs_processManager_cache_hit_count Counter	Die Anzahl der Cache-Treffer von Prozessen im System.
lfs_processManager_cache_miss_count Counter	Die Anzahl der Cache-Fehler von Prozessen im System.
lfs_blockingProcessInterceptor_cache_size Gauge	Die aktuelle Größe des Caches der Interpreter, die zum Ausführen von Prozessen verwendet werden können. Die Menge hängt von der Intensität der gestarteten Interpreter auf einem bestimmten Gerät ab. Wenn die aktuelle Größe des Dateicaches 10000 übersteigt, wird es empfohlen, den technischen Support zu kontaktieren.
lfs_blockingProcessInterceptor_cache_hit_count Counter	Anzahl der Treffer im Interpreter-Cache.
lfs_blockingProcessInterceptor_cache_miss_count Counter	Anzahl der Cache-Fehler der Interpreter.
lfs_doc_prevention_cache_file_count Gauge	Aktuelle Größe des Dateicaches der Aufgabe *Ausführungsprävention für Objekte* für Objekte, die nicht untersucht werden müssen (beim Öffnen von Dokumenten).
lfs_script_prevention_cache_file_count Gauge	Aktuelle Größe des Dateicaches der Aufgabe *Ausführungsprävention für Objekte* für Objekte, die nicht untersucht werden müssen (beim Ausführen von Skripten).
lfs_doc_prevention_cache_file_hit_count Counter	Anzahl der Treffer im Dateicache der Aufgabe *Ausführungsprävention für Objekte* für Objekte, die nicht untersucht werden müssen (beim Öffnen von Dokumenten).
lfs_script_prevention_cache_file_hit_count Counter	Anzahl der Treffer im Dateicache der Aufgabe *Ausführungsprävention für Objekte* für Objekte, die nicht untersucht werden müssen (beim Ausführen von Skripten).
lfs_doc_prevention_cache_file_miss_count Counter	Anzahl der Fehltreffer im Dateicache der Aufgabe *Ausführungsprävention für Objekte* für Objekte, die nicht untersucht werden müssen (beim Öffnen von Dokumenten).
lfs_script_prevention_cache_file_miss_count Counter	Anzahl der Fehltreffer im Dateicache der Aufgabe *Ausführungsprävention für Objekte* für Objekte, die nicht untersucht werden müssen (beim Ausführen von Skripten).
lfs_doc_prevention_cache_volume_count Gauge	Aktuelle Größe des Caches für Bereitstellungspunkte der Aufgabe „Ausführungsprävention für Objekte“ für Dokumente.
lfs_script_prevention_cache_volume_count Gauge	Aktuelle Größe des Caches für Bereitstellungspunkte der Aufgabe „Ausführungsprävention für Objekte“ für Skripte.
eka_telemetry_metrics_registry_callbacks_exec_duration_milliseconds Gauge	Die Zeit, die benötigt wurde, um das aktuelle Kennzahlen-Update durch alle im Register registrierten Clients abzuschließen (in Millisekunden).
eka_telemetry_metrics_registry_registered_callbacks Gauge	Die aktuelle Anzahl von Funktionsaufrufen zum Kennzahlen-Update, die der MetricsRegistry für alle registrierten Clients durchgeführt hat.
eka_telemetry_metrics_registry_scrape_duration_milliseconds Gauge	Die zum Erfassen der Werte aller Registrierungskennzahlen benötigte Zeit (in Millisekunden). Wenn 99% der Werte dieser Kennzahlen 10 Minuten lang größer als 1 Sekunde sind, wird es empfohlen, sich an den Technischen Support zu wenden.

Überwachung der Anwendungsstabilität

Die Überwachung der Stabilität von Kaspersky Endpoint Security verfolgt, wie oft das Programm unerwartet beendet wird, und informiert den Administrator bei instabiler Programmleistung.

So konfigurieren Sie die Überwachung der Anwendungsstabilität in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Asset-Management** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security für Linux.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Gehen Sie zur Registerkarte **Anwendungseinstellungen**.
4. Wählen Sie die Option **Allgemeine Einstellungen** → **Leistung** aus.
5. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Überwachung der Programmstabilität aktivieren**. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

So konfigurieren Sie die Überwachung der Anwendungsstabilität 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.
4. Wechseln Sie zum Abschnitt **Allgemeine Einstellungen** → **Programmeinstellungen**.
5. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Überwachung der Programmstabilität aktivieren**. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Damit die Einstellungen angewendet werden, müssen die Anwendung und der Administrationsagent neu gestartet werden.

Wenn die Anwendung instabil läuft, wird in den Eigenschaften des Geräts mit der installierten Anwendung die folgende Meldung angezeigt: *<Anzahl> ungeplanter Unterbrechungen der Anwendung seit <Datum und Uhrzeit>*.

So konfigurieren Sie die Überwachung der Programmstabilität über die Befehlszeile

In der Befehlszeile können Sie die Einstellungen zur Überwachung der Stabilität von Kaspersky Endpoint Security mithilfe der Parameter `TrackProductCrashes`, `ProductHealthLogFile`, `WarnThreshold`, `WarnAfter_#_crash` und `WarnRemovingThreshold` in der Konfigurationsdatei kesl.ini konfigurieren.

Der Parameter `TrackProductCrashes` aktiviert bei Instabilität der Anwendung das Übertragen des Gerätestatus von Kaspersky Endpoint Security an Kaspersky Security Center. Der Parameter kann die folgenden Werte annehmen:

- `Yes/true` – Aktiviert das Senden des Gerätestatus von Kaspersky Endpoint Security an Kaspersky Security Center.
- `No/false` – Deaktiviert das Senden des Gerätestatus von Kaspersky Endpoint Security an Kaspersky Security Center.

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 Anwendung 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 Anwendung entfernt wird. Standardwert: 86400 Sekunden

Mit dem Parameter `WarnAfter_#_crash` können Sie die Anzahl der Anwendungsabstürze festlegen, bei deren Überschreitung eine Benachrichtigung über eine instabile Anwendungsausführung angezeigt wird. Der Parameter kann die Werte 0 bis 10 annehmen. Standardwert: 10. Wenn der Wert auf 0 gesetzt ist, wird die keine Benachrichtigung über die Instabilität der Anwendung angezeigt.

Nachdem Sie Änderungen an dieser Datei vorgenommen haben, starten Sie Kaspersky Endpoint Security neu.

Integritätsprüfung der Anwendungskomponenten

Kaspersky Endpoint Security enthält eine Vielzahl verschiedener binärer Module in Form von dynamisch verbundenen Bibliotheken, ausführbaren Dateien, Konfigurationsdateien und Dateien der Oberfläche. Ein Hacker kann ein oder mehrere ausführbare Module oder Dateien des Programms durch andere Dateien ersetzen, die schädlichen Code enthalten. Um eine solche Ersetzung von Modulen und Dateien zu verhindern, kann Kaspersky Endpoint Security die Integrität der Programmkomponenten überprüfen. Die Anwendung überprüft Module und Dateien auf nicht autorisierte Änderungen und Schäden. Ein Modul oder eine Datei von der Anwendung mit einer nicht korrekten Prüfsumme gilt als beschädigt.

Eine Integritätsprüfung wird für die folgenden Komponenten der Anwendung durchgeführt (sofern auf dem Gerät installiert):

- Anwendungspaket.
- Paket der grafischen Benutzeroberfläche.
- Paket des Kaspersky Security Center Administrationsagenten.
- Web-Plug-in für die Verwaltung von Kaspersky Endpoint Security.
- MMC-Plug-in für die Verwaltung von Kaspersky Endpoint Security.

Die Integritätsprüfung der Anwendungskomponenten erfolgt mit dem Tool zur Integritätsprüfung. Das Tool überprüft die Integrität der Dateien, die in gesonderten Listen aufgeführt sind und *Manifestdateien* genannt werden. Jede Anwendungskomponente verfügt über ihre eigene Manifestdatei, die eine Liste von Anwendungsdateien enthält, deren Integrität für den korrekten Betrieb dieser Anwendungskomponente wichtig ist. Die Manifestdateien werden digital signiert. Auch ihre Integrität wird überprüft.

Um das Tool zur Integritätsprüfung auf Geräten mit Linux-Betriebssystemen auszuführen, ist ein Konto mit Root-Rechten erforderlich.

Das Tool zur Integritätsprüfung wird zusammen mit der Anwendung installiert und befindet sich in den folgenden Pfaden:

- Im Rahmen des Anwendungspakets (integrity_checker): /opt/kaspersky/kesl/bin/integrity_checker.
- Im Rahmen des MMC-Plug-ins zur Verwaltung von Kaspersky Endpoint Security (integrity_checker.exe):
  - Für 32-Bit-Betriebssysteme: %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<Versionsnummer>.plg\integrity_checker.exe
  - Für 64-Bit-Betriebssysteme: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<Versionsnummer>.plg\integrity_checker.exe

Die Manifestdateien finden Sie unter den folgenden Pfaden:

- Für die Integritätsprüfung des Anwendungspakets: /opt/kaspersky/kesl/bin/integrity_check.xml.
- Für die Integritätsprüfung des Pakets mit der grafische Benutzeroberfläche: /opt/kaspersky/kesl/bin/gui_integrity_check.xml.
- Um den Administrationsagenten zu überprüfen:
  - /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml – für 32-Bit-Betriebssysteme
  - /opt/kaspersky/klnagent64/bin/kl_file_integrity_manifest.xml – für 64-Bit-Betriebssysteme
- Um das MMC-Plug-in zur Verwaltung von Kaspersky Endpoint Security zu überprüfen
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<Version des Plug-ins>.plg\integrity_check.xml – für 32-Bit-Betriebssysteme
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<Version des Plug-ins>.plg\integrity_checker.xml – für 64-Bit-Betriebssysteme

Um die Integrität einer Komponente der Lösung zu überprüfen, müssen Sie das Tool im Speicherordner des Tools für diese Komponente ausführen.

Integrität des Programmpakets überprüfen

```
integrity_checker [<path to manifest file>] --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type
kds-with-filename
```

Integrität des Pakets der grafischen Benutzeroberfläche überprüfen

```
integrity_checker <path to manifest file> --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-
with-filename
```

Integrität des MMC-Verwaltungs-Plug-ins von Kaspersky Endpoint Security überprüfen

```
integrity_checker.exe [<path to manifest file>]
```

Integrität des Administrationsagenten überprüfen

```
integrity_checker <path to manifest file>
```

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 <directory>` ist der Pfad zum Verzeichnis mit der Zertifikatssperrliste.
- `--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 <file name>` schreibt die Ereignisse, die während der Untersuchung aufgetreten sind, mit der Protokollierungsstufe DEBUG in die angegebene Datei.
- `--signature-type kds` ist der zu überprüfende Signaturtyp (diese Option ist für die Überprüfung des Web-Plug-ins für die Verwaltung von Kaspersky Endpoint Security erforderlich).
- `--signature-type kds-with-filename` ist der Typ der zu überprüfenden Signatur (diese Einstellung ist für die Überprüfung des Programmpakets und des Pakets der grafischen Benutzeroberfläche erforderlich).
- `--single_file <file name>` überprüft nur die angegebene Datei im Manifest und ignoriert alle anderen Objekte des Manifests.
- `--version` – Zeigt die Version des Tools an und führt keine Integritätsprüfung aus.

Alle verfügbaren Optionen des Tools zur Integritätsprüfung anzeigen

```
integrity_checker --help
```

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 beim Starten der Anwendung ermittelt wird, dass die Integrität der Anwendung oder des Administrationsagenten verletzt ist, erstellt Kaspersky Endpoint Security ein Ereignis darüber im Ereignisprotokoll und in Kaspersky Security Center.

Zugriffssteuerung für Apps

Die Zugriffssteuerung in Kaspersky Endpoint Security basiert auf einer Role Based Access Control-Richtlinie (RBAC). Um einem Benutzer bestimmte Rechte oder Zugriff auf eine Ressource zu gewähren, müssen Sie entsprechende Rollen zuweisen. *Rolle* – Eine Reihe von Rechten und Berechtigungen zur Verwaltung der Anwendung.

Benutzerrollen erleichtern und beschleunigen die routinemäßige Verwaltung von Zugriffsrechten. Die Zugriffsrechte einer Rolle werden entsprechend den typischen Aufgaben und Stellenbeschreibungen der Benutzer konfiguriert.

Das Programm benötigt erhöhte Berechtigungen im Betriebssystem, um Geräte zu schützen. Das Programm benötigt Root-Rechte, um einige seiner grundlegenden Sicherheitsfunktionen auszuführen.

Das rollenbasierte Zugriffsmodell des Programms umfasst die Rolle „Administrator“ (admin). In bestimmten Fällen können Aktionen von Benutzern mit der Rolle „Administrator“ dazu führen, dass Vorgänge mit den Rechten des Superusers (root) des Betriebssystems ausgeführt werden.

Die Rolle „Administrator“ sollte nur vertrauenswürdigen Benutzern zugewiesen werden. Eine Kompromittierung oder ein Missbrauch der Rolle „Administrator“ führt zur Kompromittierung des gesamten Geräts und kann die Sicherheit, Integrität oder Leistung der Infrastruktur Ihrer Organisation sowie Benutzerdaten beeinträchtigen.

Die Zuweisung der Rolle „Administrator“ liegt in der Verantwortung des Systembesitzers und sollte gemäß der Zugriffssteuerungsrichtlinie Ihrer Organisation und dem Vertrauensniveau gegenüber den entsprechenden Benutzern erfolgen.

Vordefinierte Rollen

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 Anwendung.

Im Betriebssystem werden vier Gruppen von Systembenutzern erstellt:

- kesladmin
- kesluser
- keslaudit
- nokesl

Wenn Sie einem Systembenutzer eine Programmrolle zuweisen, wird der Benutzer zur entsprechenden Gruppe hinzugefügt (siehe die Tabelle unten). Wenn Sie einem Benutzer eine Rolle entziehen, wird dieser Benutzer aus der entsprechenden Gruppe entfernt.

Nachdem Sie eine Rolle zugewiesen oder entzogen haben, müssen Sie das Programm neu starten (den Prozess kesl) und seine grafische Benutzeroberfläche (den Prozess kesl-gui).

Rollen und Benutzergruppen

Rollenname	Rolle für die Anwendung	Benutzergruppe im Betriebssystem	Berechtigungen
Administrator	admin	kesladmin	Verwalten der Anwendungs- und Aufgabeneinstellungen über die grafische Oberfläche und die Befehlszeile der Anwendung, ohne Verwendung des Befehls `sudo`. Verwaltung der Lizenzierung der App beliebigen Benutzern beliebige Rollen zuweisen Benutzern Rollen entziehen (ein Administrator kann sich selbst die Rolle admin nicht entziehen). Speicher der Benutzer anzeigen und verwalten
Benutzer	user	kesluser	Nur Aufgaben für die benutzerdefinierte Untersuchung von Dateien verwalten Update-Aufgaben starten und beenden Dateien zur Untersuchung an die Sandbox senden Berichte für von Benutzern erstellte Aufgaben anzeigen Anzeigen von Ereignissen, die für alle Benutzer der Anwendung gelten
Auditor	audit	keslaudit	Einstellungen der App anzeigen Status der Anwendung anzeigen Alle Aufgaben samt Einstellungen und Zeitplänen anzeigen Alle Ereignisse anzeigen Alle Objekte im Backup anzeigen
–	–	nokesl	Keine Rolle in der Anwendung zugewiesen, es gibt keine Rechte.

Benutzerrolle zuweisen oder entziehen

Rollen legen die Rechte eines Benutzers und die Aktionen fest, die der Benutzer im System ausführen kann. Nur Benutzer mit der Rolle „Administrator“ (kesladmin) können Rollen verwalten. Es wird empfohlen, auf dem geschützten Gerät mindestens einen Benutzer mit der Rolle „Administrator“ zu erstellen, um zu verhindern, dass das Programm von Benutzern mit Root-Rechten verwaltet wird.

Liste von Benutzern und Rollen anzeigen

```
kesl-control --get-user-list
```

Einem Benutzer eine Rolle zuweisen

```
kesl-control --grant-role <admin|user|audit> <user name>
```

Beispiel für das Zuweisen der Rolle „audit“ zum Benutzer test15

```
kesl-control --grant-role audit test15
```

Einem Benutzer eine Rolle entziehen

```
kesl-control --revoke-role <role> <user name>
```

Beispiel für das Entziehen der Rolle „audit“ vom Benutzer test15

```
kesl-control --revoke-role audit test15
```

RBAC-Funktionsbereiche in Kaspersky Security Center

Standardmäßig haben Benutzer mit der Rolle „Administrator für Kaspersky Endpoint Security“ im Administrationssystem von Kaspersky Security Center Zugriff auf die gesamte Funktionalität von Kaspersky Endpoint Security.

Sie können für einen Kaspersky Endpoint Security-Benutzer oder eine Kaspersky Endpoint Security-Gruppe eine der folgenden vordefinierten Zugriffsstufen für die Funktionalität von Kaspersky Endpoint Security auswählen:

- **Lesen** berechtigt dazu, die allgemeinen Einstellungen von Kaspersky Endpoint Security und die Einstellungen der Komponenten von Kaspersky Endpoint Security anzuzeigen.
- **Bearbeiten** berechtigt dazu, die allgemeinen Einstellungen von Kaspersky Endpoint Security und die Einstellungen der Komponenten von Kaspersky Endpoint Security anzuzeigen und zu bearbeiten.
- **Ausführen** berechtigt dazu, Aufgaben von Kaspersky Endpoint Security zu starten und zu beenden.
- **Vorgänge für Geräteauswahlen ausführen** berechtigt dazu, Aufgaben von Kaspersky Endpoint Security für eine Auswahl von Geräten zu starten und zu beenden.

Sie können auch erweiterte Zugriffsberechtigungen anpassen: den Zugriff auf die Funktionen von Kaspersky Endpoint Security erlauben oder verbieten.

So konfigurieren Sie Zugriffsberechtigungen für Programmfunktionen in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Benutzer und Rollen** → **Rolle** aus.
2. Wählen Sie die Rolle aus, für die Sie Funktionsbereiche konfigurieren möchten.

   Bei Bedarf können Sie eine neue Rolle hinzufügen. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security Center.
3. Konfigurieren Sie die Zugriffsrechte für das Programm Kaspersky Endpoint Security.
4. Klicken Sie auf **Speichern**.

Zugriffsberechtigungen für Funktionen von Kaspersky Endpoint Security

Funktionsbereich	Funktionen von Kaspersky Endpoint Security
Grundfunktionen	Datenbanken und Module des Programms aktualisieren Rollback Inventar Schutz vor modifizierten USB-Geräten Überwachung der System-Integrität Prüfung der Systemintegrität Konfiguration der Erkennung Kaspersky Security Network Interaktion mit den Benutzern Leistung Netzwerkeinstellungen Container untersuchen Technischer Support Berichte und Speicher Integration mit KSC Telemetriedatenquelle und auditd-Modus (Einstellungen für die Interaktion mit dem Betriebssystem) Ereigniseinstellungen Light Agent-Modus Schlüssel hinzufügen
Programmkontrolle	Programmkontrolle
Gerätekontrolle	Gerätekontrolle
Virtuelle Datentresore	Temporären Zugriff auf ein Gerät gewähren (Gerätekontrolle)
Vertrauenswürdige Zone	Vertrauenswürdige Zone: • Gibt vertrauenswürdige Webadressen an • Vertrauenswürdige IP-Adressen • Fenster "Überwachte Ports" • Vertrauenswürdige Stammzertifikate • Vertrauenswürdige Domänen • Vertrauenswürdige Mountpunkte • Ausnahmen vom Abfangen des Datenverkehrs • Vertrauenswürdige Programme • Ausnahmen von der Schadsoftware-Untersuchung • Vertrauenswürdige Geräte

Funktionsbereich	Funktionen von Kaspersky Endpoint Security
Detection and Response	Integrierte Agenten: • Managed Detection and Response • Endpoint Detection and Response • Endpoint Detection and Response Expert (on-premises) • Endpoint Detection and Response Expert (cloud) • Network Detection and Response (KATA) • Sandbox • Integration mit KUMA. Reaktionsaktionen: • Eines Prozesses beenden • Einen Prozess starten • IOC-Untersuchung • Datei von Gerät abrufen • Datei in die Quarantäne verschieben • Datei von Gerät löschen • Netzwerkisolation • Ausführungsprävention für Objekte • Telemetrie-Einstellungen
Programm-Überwachung	Verhaltensanalyse Exploit-Prävention Schutz vor Verschlüsselung Schutz vor Netzwerkbedrohungen Firewall-Verwaltung
Schutzkomponenten	Schadsoftware-Untersuchung Untersuchung wichtiger Bereiche Komponente "Schutz vor bedrohlichen Dateien". Schutz vor E-Mail-Bedrohungen Untersuchung von Wechseldatenträgern Schutz vor Web-Bedrohungen
Web-Kontrolle	Web-Kontrolle

Empfehlungen für typische Rollen geschützter Geräte

Workstation

Wenn Sie das Programm auf einer Workstation installieren, empfehlen wir, auch die grafische Benutzeroberfläche des Programms zu installieren.

Nach der Installation des Programms:

- Aktivieren Sie den Schutz vor Web-Bedrohungen.
- Wenn das Gerät keine direkte Verbindung zum Internet hat, wählen Sie in den Einstellungen für die Untersuchung des Netzwerkverkehrs die lokale Zertifikatsprüfung mit einer der folgenden Optionen aus:
  - In der Web Console klicken Sie unter **Untersuchung verschlüsselter Verbindungen** auf die Schaltfläche **Einstellungen** und setzen Sie anschließend **Richtlinie zur Überprüfung von Zertifikaten** auf **Lokale Überprüfung**.
  - In der Verwaltungskonsole legen Sie unter **Einstellungen für verschlüsselte Verbindungen** für **Richtlinie zur Zertifikatsüberprüfung** den Wert **Lokale Prüfung** fest.

- Lokal auf dem Gerät über die Befehlszeile:

  ```
  kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
  ```

  Die Anwendung überpüft Zertifikate ohne das Internet zu verwenden.

- Konfigurieren Sie eine Ausnahme vom Abfangen von Dateioperationen (globale Ausnahme) für alle Remote-Verzeichnisse, die mit den Protokollen Samba und NFS auf dem Gerät eingebunden sind.

Dateiserver

Nach der Installation des Programms:

1. Stellen Sie sicher, dass die Untersuchung von Archiven in den Einstellungen für den Schutz vor bedrohlichen Dateien deaktiviert ist. Dieser Status gilt als Standard.
2. Erstellen Sie eine Aufgabe *Schadsoftware-Untersuchung* mit den folgenden Einstellungen:
   - Untersuchung von Archiven: aktiviert
   - Aufgabenzeitplan: während Zeiten mit minimaler Auslastung

Webserver

Kaspersky Endpoint Security ist nicht für den Schutz von Webservern vorgesehen. Zum Schutz von Webservern empfehlen wir die Verwendung von Kaspersky NGFW und Kaspersky Web Traffic Security.

Wenn Sie Kaspersky Endpoint Security auf einem Webserver verwenden, der Server das HTTPS-Protokoll nutzt und eine hohe Clientauslastung aufweist, kann der Schutz vor Web-Bedrohungen die Auslastung der Systemressourcen erheblich erhöhen. Das liegt daran, dass die Anwendung den HTTPS-Verkehr entschlüsselt und überprüft.

Analysieren Sie, wie sich die Auslastung des Webservers ändert, während der Schutz vor Web-Bedrohungen aktiv ist. Sie können Ausnahmen konfigurieren, um die Einstellungen zu optimieren und Kompatibilitätsprobleme zu vermeiden.

Proxyserver

Deaktivieren Sie nach der Installation des Programms die Komponenten Schutz vor Web-Bedrohungen und Schutz vor Netzwerkbedrohungen auf dem Gerät, das als Proxyserver oder Load Balancer fungiert.

Server mit Containerisierung

Deaktivieren Sie nach der Installation des Programms die Komponenten Schutz vor Web-Bedrohungen, Schutz vor Netzwerkbedrohungen und Firewall-Verwaltung auf Servern, die für Containerisierungsdienste verwendet werden. Für den Schutz von Container-Umgebungen kann die Anwendung Kaspersky Container Security verwendet werden.

Datenbankserver

Konfigurieren Sie globale Ausnahmen für die Arbeitsverzeichnisse des Datenbankverwaltungssystems.

Erfragen Sie bei Ihrem DBMS-Administrator die Liste der Arbeitsverzeichnisse in Ihrer Infrastruktur.

Die folgenden Beispielpfade sind für das Betriebssystem Ubuntu vorgesehen. In anderen Betriebssystemen können die Verzeichnisse abweichen.

Empfehlungen für gängige DBMS

PostgreSQL. Es ist äußerst wichtig, jegliche Latenz bei Dateioperationen mit Datendateien und Write-Ahead-Logs (WAL-Dateien) vollständig zu vermeiden. Außerdem empfehlen wir, Dateioperationen von PostgreSQL-Prozessen und Tablespaces auszuschließen (siehe Beispiel unten). In einer typischen PostgreSQL-Installation befinden sich diese Dateien in den folgenden Verzeichnissen:

- Statistiken und parallele Abfragen: `/dev/shm`
- Daten: `/var/lib/postgresql/<PostgreSQL version>/main`
- WAL-Dateien: `/var/lib/postgresql/<PostgreSQL version>/main/pg_wal`
- Ausführbare Dateien: `/usr/lib/postgresql/<PostgreSQL version>/bin/`.

Postgres Pro. Befolgen Sie die Richtlinien für PostgreSQL. Fügen Sie außerdem das Verzeichnis `/var/lib/pgpro/<Postgres Pro version>/data` zu den Ausnahmen hinzu.

Oracle Database. Eine Liste der Arbeitsverzeichnisse für alle Datenbanken können Sie der Konfigurationsdatei `/etc/oratab` entnehmen.

ScyllaDB. Wenn Sie die Komponenten Schutz vor Web-Bedrohungen und Schutz vor Netzwerkbedrohungen verwenden, verwenden Sie den eBPF-Modus zum Abfangen des Datenverkehrs. Um den Caching-Modus von Detection and Response-Lösungen zu verwalten, verwenden Sie den Standardwert der Einstellung `UseIncreasedXdrEventsCache=yes` in der Konfigurationsdatei kesl.ini.

Beispiel für die Konfiguration globaler Ausnahmen für PostgreSQL-Arbeitsverzeichnisse

Wenn Sie zum Abfangen von Systemereignissen einen auf der *fanotify-Technologie* basierenden Mechanismus verwenden, müssen die DBMS-Dateiverzeichnisse Mount-Punkte sein. Wenn Sie das *aktualisierbare Kernel-Modul* zum Abfangen von Systemereignissen verwenden, müssen Sie keine Mount-Punkte erstellen.

So erstellen Sie Mount-Punkte:

1. Prüfen Sie, ob die Verzeichnisse mit der Datenbankdatei Mount-Punkte sind:

   ```
   mount
   ```

Wenn die Verzeichnisse in der Ausgabe des Befehls mount nicht aufgeführt sind:

a. Erstellen Sie einen Einhängepunkt:

```
mount --bind /var/lib/postgresql/<PostgreSQL version>/main/ /var/lib/postgresql/<PostgreSQL version>/main
```

Sie müssen keinen separaten Mount-Punkt für das Verzeichnis mit den WAL-Dateien erstellen, da es im Datenverzeichnis verschachtelt ist.

b. Fügen Sie der Datei /etc/fstab die folgende Zeile hinzu, damit der neu erstellte Einhängepunkt nach dem Neustart im System erhalten bleibt:

```
/var/lib/postgresql/<PostgreSQL version>/main /var/lib/postgresql/<PostgreSQL version>/main none
defaults,bind 0 0
```

2. Starten Sie den PostgreSQL-Dienst neu:

```
systemctl restart postgresql
```

So konfigurieren Sie globale Ausnahmen für Arbeitsverzeichnisse:

1. Fügen Sie die Verzeichnisse zu den globalen Ausnahmen hinzu:

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000=/var/lib/postgresql/<PostgreSQL version>/main
kesl-control --set-app-settings ExcludedMountPoint.item_0001=/var/lib/postgresql/<PostgreSQL
version>/main/pg_wal
kesl-control --set-app-settings ExcludedMountPoint.item_0002=/usr/lib/postgresql/<PostgreSQL version>/bin/
kesl-control --set-app-settings ExcludedMountPoint.item_0003=/usr/lib/postgresql/<PostgreSQL version>
```

2. Wenn Sie Tablespaces verwenden, fügen Sie diese ebenfalls zu den Ausnahmen hinzu:

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000=<tablespace directory>
```

3. Starten Sie die Anwendung neu, um die globalen Ausnahmen anzuwenden:

```
systemctl restart kesl
```

Datenbanken und Module des Programms aktualisieren

Ein Update der Datenbanken und Module von Kaspersky Endpoint Security gewährleistet, dass der Schutz Ihres Geräts auf dem neuesten Stand ist. Jeden Tag tauchen neue Viren und andere Schadprogramme auf. Informationen über Bedrohungen und entsprechende Neutralisierungsmethoden sind in den Datenbanken von Kaspersky Endpoint Security enthalten. 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 Anwendung erforderlich. Wenn Sie über keine gültige Lizenz verfügen, können Sie nur ein Mal ein Update durchführen.

Wenn die Programmbereitstellung erfolgreich war und Sie bei der Erstkonfiguration die Aktualisierung der Datenbanken ausgewählt haben, sind die Datenbanken nach der Installation des Programms auf dem neuesten Stand. Informationen zum Status der Datenbanken erhalten Sie beim Anzeigen des Schutzstatus des Geräts in Kaspersky Security Center anhand der Status der Client-Geräte sowie in der Befehlszeile mithilfe des Befehls `kesl-control --app-info`. Wenn die Datenbanken nicht auf dem neuesten Stand sind, müssen Sie ein Datenbanken-Update konfigurieren und starten.

Konfigurieren von Datenbank- und Modul-Updates

1. **Auswählen eines Update-Verteilungsschemas und einer Update-Quelle**

   Update-Quelle – Eine Ressource, die Datenbanken-Updates und Updates der Module der Anwendung Kaspersky Endpoint Security enthält. Als Update-Quelle kann Folgendes dienen: Kaspersky-Update-Server; Speicher des Kaspersky Security Center Administrationsservers; ein FTP-, HTTP- oder HTTPS-Server; ein lokales Verzeichnis oder Netzwerkverzeichnis, das vom Benutzer mithilfe der Protokolle Samba oder NFS eingehängt wurde.

   > Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, werden die Datenbanken auf den geschützten virtuellen Maschinen aus dem Verzeichnis auf der SVM aktualisiert.

2. **Konfigurieren der Aufgabe zum Datenbanken-Update**

   Die Aufgabe *Update* lädt das Update-Paket herunter und installiert Updates für Datenbanken und Programm-Module auf dem Gerät.

Die Funktionen zur Aktualisierung (einschließlich Updates des Anti-Virus-Signaturen und der Codebase) und für KSN sind in dieser Anwendung in den USA möglicherweise nicht verfügbar.

Während der Durchführung eines Updates werden die folgenden Objekte heruntergeladen und auf Ihrem Gerät installiert:

- Datenbanken für Kaspersky Endpoint Security. Die Programm-Datenbanken enthalten Regeln zur Erkennung von Malware, eine Beschreibung von Netzwerkangriffen, Datenbanken für schädliche Webadressen und Phishing-Webadressen, Datenbanken für Banner, Spam-Datenbanken sowie andere Daten.
- Programm-Module. Modul-Updates dienen dazu, Schwachstellen in der Anwendung zu beseitigen und die Schutztechniken für das Gerät zu verbessern. Bei Modul-Updates kann das Verhalten von Programmkomponenten geändert und neue Funktionen können hinzugefügt werden.

Sie können auch automatisch installierbare Anwendungsupdates (Autopatches) abrufen. Autopatches enthalten Korrekturen und Verbesserungen für das Programm.

Bei der Aktualisierung werden die Programm-Module und Datenbanken auf Ihrem Computer mit ihren aktuellen Versionen 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 Updatepaket groß sein, was zu zusätzlichem Internet-Datenverkehr (bis zu mehreren MB) führen kann. Der Umfang des erforderlichen Speicherplatzes kann bis zu 3 GB betragen.

Nützliche Artikel

Behebung von Problemen mit Updates für Programm-Datenbanken und -Module

Was tun, wenn der folgende Status angezeigt wird: „Ein Programm-Update oder ein Update des cryptossl-Moduls wurde installiert. Starten Sie das Programm neu.“

Auswählen der Update-Quelle und des Verteilungsschemas

Auswählen einer Update-Quelle für Kaspersky Endpoint Security

Update-Quelle – Eine Ressource, die Datenbanken-Updates und Updates der Module der Anwendung Kaspersky Endpoint Security enthält.

Als Update-Quelle können die Kaspersky-Update-Server, der Speicher des Kaspersky Security Center Administrationsservers, ein vom Benutzer eingebundenes lokales Verzeichnis oder Netzwerkverzeichnis (SMB/NFS) sowie FTP-, HTTP- oder HTTPS-Server dienen. Wenn Sie Ihren eigenen HTTPS-Server als Update-Quelle auswählen, müssen Sie sicherstellen, dass dieser über die richtige Zertifikatskette verfügt. Ein selbstsigniertes Zertifikat kann nur als Stammzertifikat in einer Zertifikatskette verwendet werden. In diesem Fall müssen Sie es zur Liste der vertrauenswürdigen Zertifikate auf dem Gerät hinzufügen.

Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, werden die Datenbanken auf den geschützten virtuellen Maschinen aus dem Verzeichnis auf der SVM aktualisiert.

Wurden mehrere Ressourcen als Update-Quellen gewählt, versucht Kaspersky Endpoint Security, der Reihenfolge in der Liste von oben nach unten nach eine Verbindung zu ihnen herzustellen, und führt die Update-Aufgabe aus, indem es das Update-Paket aus der ersten verfügbaren Quelle abruft. Sie können die Wartezeit auf eine Antwort von der ausgewählten Update-Quelle konfigurieren, die beim Versuch gilt, eine Verbindung zu dieser Quelle herzustellen. Wenn in der angegebenen Zeit keine Antwort von der Update-Quelle eingeht, greift die App auf eine andere angegebene Update-Quelle zu.

Auswählen eines Verteilungsschemas für Updates

Kaspersky Endpoint Security unterstützt die folgenden Verteilungsschemata für Updates von Datenbanken und Programm-Modulen:

Zentralisiertes Update

Wenn Sie Kaspersky Security Center verwenden, um den Geräteschutz in Ihrem Unternehmen zentral zu verwalten, wird empfohlen, zentrale Datenbanken-Updates einzurichten. Das zentralisierte Update gewährleistet eine Reduzierung des externen Internet-Datenverkehrs und eine bequeme Kontrolle des Updates.

Das zentralisierte Update besteht aus den folgenden Schritten:

1. Laden Sie das Update-Paket in ein Repository im Unternehmensnetzwerk herunter.

   Als Speicher können Sie die Datenverwaltung des Administrationsservers von Kaspersky Security Center verwenden. Das Update-Paket wird über die Administrationsserver-Aufgabe *Updates in die Datenverwaltung des Administrationsservers herunterladen* in die Datenverwaltung des Administrationsservers heruntergeladen.

2. Verteilen Sie das Update-Paket an die Client-Geräte.

   Das Update-Paket wird von der *Update*-Aufgabe der Anwendung Kaspersky Endpoint Security an die Client-Geräte verteilt. Wählen Sie in den Aufgabeneinstellungen Kaspersky Security Center als Update-Quelle aus.

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 Anwendung zum nächsten Server. Die Updates werden über das HTTPS-Protokoll heruntergeladen. Weitere Informationen zu Kaspersky-Update-Servern finden Sie in der Wissensdatenbank des Technischen Supports.

Update aus einem lokalen Verzeichnis oder Netzwerkverzeichnis (SMB/NFS), das von einem Benutzer gemountet wurde, oder von einem FTP-, HTTP- oder HTTPS-Server

Die benutzerdefinierte Update-Quelle muss vorab heruntergeladene Update-Pakete enthalten (diese können Sie beispielsweise mithilfe des Dienstprogramms Kaspersky Update Utility herunterladen). Wenn Sie Ihren eigenen HTTPS-Server als Update-Quelle auswählen, müssen Sie sicherstellen, dass dieser über die richtige Zertifikatskette verfügt. Ein selbstsigniertes Zertifikat kann nur als Stammzertifikat in einer Zertifikatskette verwendet werden. In diesem Fall müssen Sie es zur Liste der vertrauenswürdigen Zertifikate auf dem Gerät hinzufügen. Sie können eine benutzerdefinierte Update-Quelle in den Einstellungen der Aufgabe *Update* angeben. Weitere Informationen zum Erstellen benutzerdefinierter Update-Quellen finden Sie in der Hilfe zu Kaspersky Security Center.

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 Proxyserver verwenden, geben Sie die Proxyserver-Einstellungen an.

Aufgabe zum Datenbanken-Update konfigurieren

Die Aufgabe *Update* lädt das Update-Paket herunter und installiert Updates für Datenbanken und Programm-Module auf dem Gerät.

Datenbanken in Kaspersky Security Center aktualisieren

In Kaspersky Security Center wird die Aufgabe *Update* automatisch vom Schnellstartassistenten des Administrationsservers erstellt. Um die Aufgabe *Update* während der Ausführung des Assistenten zu erstellen, müssen Sie das Verwaltungs-Plug-in für Kaspersky Endpoint Security installieren.

Sie können eine automatisch erstellte Gruppenaufgabe *Update* verwenden oder benutzerdefinierte Gruppenaufgaben und lokale Aufgaben für Updates mithilfe der Web Console oder der Verwaltungskonsole erstellen und ausführen.

Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, werden Datenbanken auf geschützten virtuellen Maschinen mithilfe einer speziellen lokalen Aufgabe *Update* aktualisiert, bei der das Verzeichnis auf der SVM als Update-Quelle angegeben ist. Diese Update-Aufgabe wird automatisch gestartet. Sie können diese Aufgabe weder löschen noch ihre Einstellungen ändern. Das Aktualisieren von Datenbanken und Modulen der Anwendung mithilfe von Aufgaben, die in Kaspersky Security Center erstellt wurden, wird nicht unterstützt.

Update-Aufgabe in der Web Console konfigurieren und starten

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Wählen Sie in der Aufgabenliste die Update-Aufgabe für Kaspersky Endpoint Security aus und klicken Sie auf den Namen der Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wählen Sie im Abschnitt **Update-Quellen** je nach verwendetem Update-Szenario die Quelle aus, aus der das Programm Updates für Datenbanken und Module bezieht.

   Die Liste mit Update-Quellen enthält zwei Quellen: die Kaspersky-Update-Server und Kaspersky Security Center. In der Spalte **Status** wird angezeigt, ob die Anwendung diese Update-Quelle beim Ausführen der Aufgabe verwendet. Sie können der Liste weitere Update-Quellen hinzufügen, indem Sie auf die Schaltfläche **Hinzufügen** klicken. Als Update-Quellen können Sie Verzeichnisse auf FTP-, HTTP- und HTTPS-Servern oder Verzeichnisse auf beliebigen Geräten angeben, die auf dem geschützten Client-Gerät gemountet sind, einschließlich Verzeichnissen auf Remote-Geräten, die über die Protokolle Samba oder NFS gemountet sind. Wenn ein Update aus einer bestimmten Update-Quelle nicht durchgeführt werden kann, verbindet sich Kaspersky Endpoint Security mit der nächsten Quelle. Die Anwendung wendet sich der Reihe nach so an die Update-Quellen, wie sie in der Tabelle platziert wurden.

5. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Zeitplan** aus und konfigurieren Sie den Zeitplan für die Ausführung der Update-Aufgabe. Standardmäßig ist für die Aufgabe der manuelle Start ausgewählt.

   Wenn Sie **Kaspersky Security Center** als Update-Quelle ausgewählt haben, wählen Sie in der Dropdown-Liste **Aufgabenstart** die Option **Wenn Updates in den Speicher heruntergeladen werden** aus. Weitere Informationen zur Planung von Aufgaben finden Sie in der Hilfe zu Kaspersky Security Center.

6. Speichern Sie die vorgenommenen Änderungen.

Die Aufgabe wird gemäß dem konfigurierten Zeitplan gestartet. Die Aufgabe kann auch manuell gestartet werden.

Update-Aufgabe in der Verwaltungskonsole konfigurieren und starten

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 eine 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 in der Tabelle je nach verwendetem Update-Szenario die Update-Quelle aus, aus der die Anwendung je nach Update-Schema die Updates für die Datenbanken und Modul bezieht.

   Die Liste mit Update-Quellen enthält zwei Quellen: die Kaspersky-Update-Server und Kaspersky Security Center. In der Spalte **Status** wird angezeigt, ob die Anwendung diese Update-Quelle beim Ausführen der Aufgabe verwendet. Sie können der Liste weitere Update-Quellen hinzufügen, indem Sie auf die Schaltfläche **Hinzufügen** klicken. 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 Anwendung 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 die Registerkarte **Zeitplan** aus und konfigurieren Sie den Zeitplan für die Ausführung der Update-Aufgabe. Standardmäßig ist für die Aufgabe der manuelle Start ausgewählt.

   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. Weitere Informationen zur Planung von Aufgaben 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. Die Aufgabe kann auch manuell gestartet werden.

Datenbanken über die Befehlszeile aktualisieren

Über die Befehlszeile können Sie Datenbanken und Programm-Module mithilfe der *`Update`* vordefinierten Aufgabe aktualisieren oder Benutzeraufgaben vom Typ `Update` erstellen.

Sie können manuelle Update-Aufgaben verwalten (starten, beenden, anhalten und fortsetzen), den Aufgabenzeitplan konfigurieren und Update-Einstellungen durch Ändern der Einstellungen von Aufgaben verwalten.

Update-Aufgabe über die Befehlszeile erstellen und konfigurieren

Über die Befehlszeile können Sie eine benutzerdefinierte Update-Aufgabe auf zwei Arten erstellen und konfigurieren:

- Erstellen Sie eine Aufgabe, indem Sie alle Einstellungen der Aufgabe in einer Konfigurationsdatei angeben.
- Erstellen Sie eine Aufgabe mit Standardeinstellungen und konfigurieren Sie anschließend ihre Einstellungen.

Update-Aufgabe mit Einstellungen aus einer Konfigurationsdatei erstellen

```
kesl-control --create-task <task name> --type <task type> --file <path to file> [--json]
```

Wobei gilt:

- `<path to file>` ist der vollständige Pfad zur Konfigurationsdatei mit den Einstellungen, die Sie für die Aufgabe verwenden möchten.
- `--json` wird angegeben, um die Einstellungen aus der Konfigurationsdatei im JSON-Format zu importieren. Wenn Sie den Schalter `--json` nicht angeben, versucht die Anwendung, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Beispiel einer Konfigurationsdatei

```
ConnectionTimeout=10
ApplicationUpdateMode=DownloadOnly
[Sources.item_0000]
Enabled=Yes
SourceType=Custom
URL=https://s00.upd.kaspersky.com
```

So erstellen und konfigurieren Sie eine Update-Aufgabe mit Standardeinstellungen:

1. Erstellen Sie eine Aufgabe, indem Sie den folgenden Befehl ausführen:

   ```
   kesl-control --create-task <update task name> --type Update
   ```

   Dabei ist `<update task name>` der Name, den Sie für die neue Update-Aufgabe festlegen möchten.

   Dieser Befehl erstellt eine Update-Aufgabe mit Standardeinstellungen.

2. Verwalten Sie bei Bedarf die Einstellungen der Update-Aufgabe, indem Sie den folgenden Befehl ausführen:

   ```
   kesl-control --set-settings <update task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

3. Verwalten Sie bei Bedarf die Zeitplaneinstellungen der Update-Aufgabe, indem Sie den folgenden Befehl ausführen:

   ```
   kesl-control --set-schedule <update task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

4. Überprüfen Sie die aktuellen Werte der Aufgabeneinstellungen, indem Sie den folgenden Befehl ausführen:

   ```
   kesl-control --get-settings <update task ID|name>
   ```

Datenbanken in der grafischen Oberfläche des Programms aktualisieren

Update-Aufgabe über die grafische Benutzeroberfläche starten oder stoppen

1. Öffnen Sie das Hauptfenster der grafischen Benutzeroberfläche des Programms.
2. Klicken Sie im Hauptfenster der Anwendung 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 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 aktualisieren Sie 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 in Kaspersky Security Center 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. Ausführliche Informationen über die Verwendung von Kaspersky Update Utility finden Sie in der Kaspersky-Wissensdatenbank.
3. Konfigurieren Sie das Update der Datenbanken und Module der Anwendung aus dem angegebenen freigegebenen Verzeichnis auf den übrigen Geräten im lokalen Unternehmensnetzwerk.

   a. Öffnen Sie über Web Console oder die Verwaltungskonsole die Eigenschaften der Aufgabe **Update**, die auf dem erforderlichen Gerät ausgeführt wird.

   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.

d. Klicken Sie in der Tabelle der Update-Quellen auf die Schaltfläche **Hinzufügen** und geben Sie den Pfad zum freigegebenen Verzeichnis an.

> Die Adresse der Update-Quelle muss mit der in den Einstellungen von Kaspersky Update Utility angegebenen Adresse übereinstimmen.

e. Aktivieren Sie das Kontrollkästchen **Diese Quelle verwenden** und klicken Sie auf **OK**.

f. Legen Sie in der Tabelle der Update-Quellen mit den Schaltflächen **Nach oben** und **Nach unten** die Reihenfolge fest, in der sie verwendet werden.

g. Speichern Sie die Änderungen an den Aufgabeneinstellungen.

So konfigurieren Sie über die Befehlszeile 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. Ausführliche Informationen über die Verwendung von Kaspersky Update Utility finden Sie in der Kaspersky-Wissensdatenbank.

3. Konfigurieren Sie Updates der Programmdatenbanken und -module aus dem angegebenen freigegebenen Verzeichnis auf anderen Geräten im lokalen Netzwerk des Unternehmens: Legen Sie in den Update Aufgabeneinstellungen `SourceType=Custom` fest und geben Sie im Abschnitt `[Sources.item_#]` den Pfad zum freigegebenen Verzeichnis an.

   > Die Adresse der Update-Quelle muss mit der in den Einstellungen von Kaspersky Update Utility angegebenen Adresse übereinstimmen.

So führen Sie ein Rollback für Updates der Programmdatenbanken und -module durch

Nach dem zweiten Update der Datenbanken und Programm-Module steht eine Rollback-Funktion zur Verfügung, mit der Sie zu den vorherigen Versionen der Datenbanken und Programm-Module zurückkehren können.

Jedes Mal, wenn der Benutzer das Update startet, erstellt Kaspersky Endpoint Security zuerst eine Backup-Kopie der bisher verwendeten Datenbanken und Programm-Module und beginnt dann mit der Aktualisierung. Somit kann bei Bedarf zur Verwendung der vorherigen Datenbanken und Programm-Module zurückgekehrt werden. Die Rollback-Funktion für das letzte Update ist beispielsweise nützlich, wenn die neue Datenbankversion einen Fehlalarm auslöst, durch den Kaspersky Endpoint Security eine harmlose Anwendung blockiert.

Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, kann die Aufgabe nicht für das Rollback von Datenbanken-Updates verwendet werden.

In Kaspersky Security Center können Sie über die Web Console oder die Verwaltungskonsole Rollback-Aufgaben für Administrationsgruppen oder einzelne Geräte erstellen.

Über die Befehlszeile können Sie ein Datenbanken-Update auf folgende Arten zurücksetzen:

- Führen Sie die vordefinierte Aufgabe *Rollback* aus.
- Erstellen und starten Sie eine benutzerdefinierte Aufgabe *Rollback*.

Die Aufgabe *Rollback des Datenbanken-Updates* hat keine Einstellungen.

So führen Sie in der Web Console ein Rollback für ein Update der Programmdatenbanken und -module aus

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.
   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf **Hinzufügen**.
   Der Assistent für neue Aufgaben wird gestartet.
3. Passen Sie die Einstellungen der Aufgabe an:
   a. Wählen Sie in der Dropdown-Liste **Anwendung** den Namen des Programms aus.
   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Rollback**.
   c. Geben Sie im Feld **Aufgabenname** einen Namen für die neue Aufgabe ein.
   d. Wählen Sie unter **Geräte, denen die Aufgabe zugewiesen wird** aus, wie Sie einen Gültigkeitsbereich für die Aufgabe festlegen möchten.
4. Wählen Sie die Geräte entsprechend Ihrer bevorzugten Methode zum Festlegen des Aufgabenbereichs aus.
5. Schließen Sie den Assistenten ab.
   Die neue Aufgabe wird in der Aufgabenliste angezeigt.
6. Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Starten**.

So führen Sie in der Verwaltungskonsole ein Rollback für ein Update der Programmdatenbanken und -module aus

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 in der Liste Kaspersky Endpoint Security und den Aufgabentyp **Rollback** aus.

3. Wenn Sie eine Aufgabe für mehrere Geräte erstellen, fordert der Assistent Sie auf, die Geräte auszuwählen, denen Sie die Aufgabe zuweisen möchten. Wählen Sie aus, wie Sie den Aufgabenbereich definieren möchten.

4. Wählen Sie die Geräte entsprechend Ihrer bevorzugten Methode zum Festlegen des Aufgabenbereichs aus.

5. Konfigurieren Sie einen Zeitplan für die Aufgabe.

6. Geben Sie einen Namen für die neue Aufgabe ein.

7. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

8. Wählen Sie in der Aufgabenliste die Aufgabe aus, öffnen Sie das Kontextmenü der Aufgabe und wählen Sie **Starten** aus.

So führen Sie über die Befehlszeile ein Rollback für ein Update der Programmdatenbanken und -module aus

Führen Sie den Befehl aus:

```
Rollback von Datenbanken- und Modul-Updates durchführen
```

```
kesl-control --start-task 7
```

So führen Sie in der grafischen Benutzeroberfläche ein Rollback für ein Update der Programmdatenbanken und -module aus

1. Öffnen Sie das Hauptfenster der grafischen Benutzeroberfläche des Programms.

2. Klicken Sie im Hauptfenster der Anwendung auf die Schaltfläche **Update**.

   Das Fenster **Update** wird geöffnet.

3. Klicken Sie auf den Link **Update zurücksetzen**, um das Datenbanken-Update zurückzusetzen.

Geräteschutz vor Bedrohungen

Schutz vor bedrohlichen Dateien

Der Schutz vor bedrohlichen Dateien bietet ein Mindestmaß an Sicherheit für den Computer. Die Komponente wird zusammen mit Kaspersky Endpoint Security gestartet und untersucht Dateien in Echtzeit.

Funktionsweise des Schutzes vor bedrohlichen Dateien

1. **Das Programm fängt Ereignisse von Dateioperationen ab und blockiert Aktionen, bis die Untersuchung abgeschlossen ist.**

   Das Programm verwendet einen Mechanismus zum Abfangen von Dateioperationen und blockiert jeglichen Zugriff auf die Datei, bis die Untersuchung abgeschlossen ist.

2. **Das Programm untersucht die Datei**

   Der Schutz vor bedrohlichen Dateien untersucht eine Datei mithilfe der folgenden Technologien:

   - Antiviren-Datenbanken.
   - Cloud-Dienste von Kaspersky Security Network.
   - Die Technologie der heuristischen Analyse ermöglicht die Erkennung von Bedrohungen, die noch nicht in den Kaspersky-Datenbanken erfasst sind.

3. **Abschluss der Untersuchung**

   Nach der Untersuchung erlaubt das Programm entweder den Vorgang oder blockiert ihn und führt die beim Fund einer Bedrohung angegebene Aktion aus.

Erstkonfiguration des Schutzes vor bedrohlichen Dateien

Die Erstkonfiguration umfasst die notwendigen Schritte für den grundlegenden Schutz von Endgeräten.

1. **Wählen Sie einen Mechanismus zum Abfangen von Systemereignissen aus**

   Der Schutz vor bedrohlichen Dateien fängt Ereignisse von Dateioperationen ab und blockiert Aktionen, bis die Untersuchung abgeschlossen ist.

   Bei der Installation des Programms haben Sie einen Mechanismus zum Abfangen von Systemereignissen ausgewählt:

   - Abfangmechanismus auf Basis des aktualisierbaren Kernel-Moduls
   - System-Abfangmechanismus auf Basis von fanotify
   - Kernel-Modul für den Schutz vor bedrohlichen Dateien auf einem Betriebssystem ohne fanotify

Die Wahl des Mechanismus zum Abfangen von Systemereignissen hängt von der Konfiguration des Computers ab. Die Abfangtechnologie, die die höchste Leistung bietet, ist das aktualisierbare Kernel-Modul. Sie können diesen Mechanismus in den Programmeinstellungen aktivieren.

2. **Schutz vor bedrohlichen Dateien konfigurieren**

   Der Schutz vor bedrohlichen Dateien ist standardmäßig aktiviert und wird mit den von Kaspersky-Experten empfohlenen Einstellungen ausgeführt. Die Standardeinstellungen bieten das empfohlene Schutzniveau und eine optimale Ressourcennutzung. Wenn Sie besondere Anforderungen an die Sicherheit der Infrastruktur haben, können Sie diese Einstellungen ändern.

3. **Schutzbereich konfigurieren**

   Standardmäßig untersucht das Programm alle Dateien auf einem geschützten Gerät. Wenn Sie nur ein einzelnes Verzeichnis untersuchen müssen (z. B. das Verzeichnis, in das Dateien automatisch aus einer externen Quelle heruntergeladen werden), können Sie nur dieses Verzeichnis als Schutzbereich festlegen. In anderen Fällen empfehlen wir, den Standardschutzbereich beizubehalten und Ausnahmen zu verwenden, um den Bereich gezielt anzupassen.

4. **Mount-Punkte von der Untersuchung ausschließen**

   Wenn Sie Mount-Punkte von der Untersuchung ausschließen, fängt das Programm Dateivorgänge in einem bestimmten Verzeichnis nicht ab. Sie können beispielsweise gemeinsam genutzte Netzwerkressourcen von der Untersuchung ausschließen und sie mithilfe von Kaspersky Endpoint Security auf dem Gerät schützen, auf dem diese Ressourcen physisch gespeichert sind. Sie können auch die Empfehlungen für den Schutz vor bedrohlichen Dateien und Untersuchungsaufgaben zurate ziehen.

5. **Ausnahmen hinzufügen**

   Ausnahmen helfen dabei, Systemsicherheit und Leistung in Einklang zu bringen. Für einen stabilen Betrieb von Drittanbieter-Software fügen Sie Dateien und Verzeichnisse zu den Ausnahmen hinzu, die in der Dokumentation der jeweiligen Software aufgeführt sind.

   Es wird empfohlen, die folgenden Objekte auszuschließen:

   - Datenbanken. Die Untersuchung großer Datenbanken erfordert viele Ressourcen. Häufiger Zugriff auf Datenbankdateien löst häufige Untersuchungen aus.
   - Dateien, mit denen ressourcenintensive Prozesse arbeiten. Die Untersuchung solcher Dateien verlangsamt den Computer.
   - Verzeichnisse mit Protokolldateien. Das Betriebssystem schreibt ständig in die Protokolldatei. Infolgedessen verbraucht der Schutz vor bedrohlichen Dateien Computerressourcen unnötig für die Untersuchung von Protokolldateien.

   Wenn ein Objekt von der Untersuchung durch die Komponente „Schutz vor bedrohlichen Dateien“ ausgeschlossen ist, wird empfohlen, solche Objekte mit der Aufgabe *Schadsoftware-Untersuchung* zu untersuchen.

Zusätzliche Konfiguration für Server mit hoher Auslastung

Die zusätzliche Konfiguration umfasst Schritte zur Feinabstimmung des Schutzes vor bedrohlichen Dateien. Wenn nach der Erstkonfiguration Verzögerungen auftreten oder wenn Sie Server mit hoher Auslastung konfigurieren, gehen Sie folgendermaßen vor:

1. **Blockierung des Dateizugriffs während der Untersuchung deaktivieren**

   Standardmäßig blockiert der Schutz vor bedrohlichen Dateien den gesamten Zugriff auf die zu untersuchende Datei, bis die Untersuchung abgeschlossen ist. Wenn Sie den Blockierungsmodus deaktivieren, arbeitet der Schutz vor bedrohlichen Dateien im Modus „Informieren“. Diese Art des Abfangens von Dateivorgängen wirkt sich weniger stark auf die Systemleistung aus. Allerdings werden in diesem Fall in Dateien gefundene Bedrohungen weder desinfiziert noch gelöscht. Sie können die Aufgabe Schadsoftware-Untersuchung ausführen, um solche Bedrohungen später zu verarbeiten.

   > Wenn der Blockierungsmodus deaktiviert ist, arbeiten auch Gerätekontrolle, die Aktion Ausführungsprävention für Objekte und die Aufgabe Untersuchung von Wechseldatenträgern im Modus „Informieren“.

2. **Statistiken zur Dateiuntersuchung erfassen**

   Überwachen Sie die wichtigsten Leistungskennzahlen des Computers: die CPU-Auslastung, die Leistung von Drittanbieter-Software oder andere Indikatoren. So können Sie ermitteln, wie sich die Systemlast reduzieren lässt.

   Sie können Statistiken zur Dateiuntersuchung mithilfe von Tools zur Analyse der Programmleistung abrufen. Sie können auch eigene Überwachungstools verwenden.

3. **Programmleistung optimieren**

   Optimieren Sie nach der Analyse der gesammelten Informationen die Leistung des Programms:

   - Globale Ausnahmen hinzufügen
   - Ausnahmen hinzufügen
   - Programmeinstellungen optimieren

4. **Blockierung des Dateizugriffs während der Untersuchung aktivieren**

   Aktivieren Sie die Blockierung des Dateizugriffs während der Untersuchung. Wenn ein infiziertes Objekt erkannt wird, wird das Programm die ausgewählte Aktion ausführen.

Besonderheiten und Einschränkungen

- Wenn der Root-Benutzer keinen Zugriff auf eine Datei in einem Remote-Verzeichnis hat, das über das NFS4-Protokoll auf dem Gerät eingebunden ist, blockiert das Programm den Zugriff auf diese Datei für alle Benutzer.
- Wenn der Schutz vor bedrohlichen Dateien und Container-Überwachung aktiviert sind, untersucht das Programm auch alle Namespaces und Container.

So erstellen Sie einen Schutzbereich

Ein *Schutzbereich* ist eine Liste mit Pfaden zu Objekten, die Kaspersky Endpoint Security auf Bedrohungen untersucht. Standardmäßig untersucht das Programm alle Dateien auf einem geschützten Gerät. Wenn Sie nur ein einzelnes Verzeichnis untersuchen möchten (z. B. das Verzeichnis, in das Dateien automatisch aus einer externen Quelle heruntergeladen werden), können Sie dieses Verzeichnis als Schutzbereich angeben. In anderen Fällen empfehlen wir, den Standardschutzbereich beizubehalten und Ausnahmen zu verwenden, um den Bereich gezielt anzupassen.

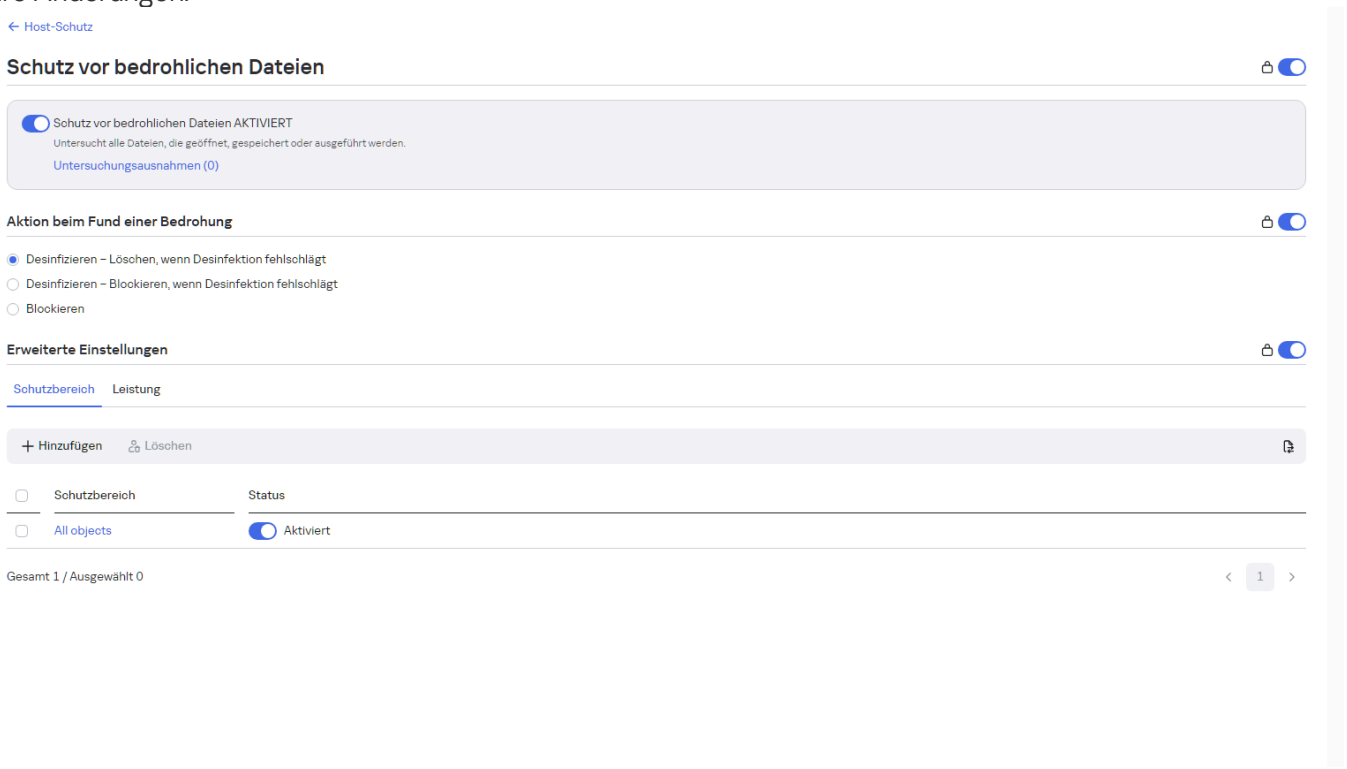
Kaspersky Endpoint Security untersucht Objekte in der Reihenfolge, in der sie in der Liste der Objekte aufgeführt sind. Um bei Bedarf für das Unterverzeichnis andere Sicherheitseinstellungen festzulegen als für das übergeordnete Verzeichnis, platzieren Sie erforderlichenfalls das Unterverzeichnis in der Liste über dem übergeordneten Verzeichnis.

So erstellen Sie einen Schutzbereich in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Schutz vor bedrohlichen Dateien**.
5. Klicken Sie im Block **Schutzbereich** auf **Hinzufügen**.
6. Daraufhin wird ein Fenster geöffnet; wählen Sie in diesem Fenster den Typ des Dateisystems aus:
   - **Lokal**. Verzeichnisse auf der Festplatte, auf die ohne Netzwerkverbindung zugegriffen werden kann.
   - **Eingehängt**. Eingebundene Remote- oder lokale Verzeichnisse.
   - **Freigegeben**. Computerverzeichnisse, auf die über das Samba- (SMB) oder das NFS-Protokoll zugegriffen werden kann.
   - **Alle remote eingehängten**. Alle Remote-Verzeichnisse, die auf dem Gerät über die Protokolle Samba und NFS eingebunden sind.
   - **Alle freigegebenen**. Alle Computerverzeichnisse, auf die über die Protokolle Samba und NFS zugegriffen wird.
7. Geben Sie für ein lokales Dateisystem einen Verzeichnispfad an (z. B. `/path/to/folder`). Aktivieren Sie bei Bedarf das Kontrollkästchen **Unterordner einschließen**.
8. Geben Sie das Zugriffsprotokoll für ein eingebundenes oder freigegebenes Dateisystem an.
9. Geben Sie Masken für Objekterweiterungen an (z. B. `*.txt`). Trennen Sie die Masken durch Kommas.

10. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Komponente "Schutz vor bedrohlichen Dateien".

So erstellen Sie einen Schutzbereich über die Befehlszeile

1. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control --set-settings 1 --add-path <path>
   ```

   Den Aufgabeneinstellungen wird ein neuer Abschnitt vom Typ `[ScanScope.item_#]` hinzugefügt. Die Anwendung untersucht die Objekte im Verzeichnis, das im Parameter `Path` angegeben ist.

2. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --get-settings 1
   ```

Beispiel

```
kesl-control --set-settings 1 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

Die folgenden Einstellungen für den Schutzbereich werden der Aufgabe hinzugefügt:

```
[ScanScope.item_0001]
AreaDesc=All object
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

So wählen Sie eine Aktion beim Erkennen einer Dateibedrohung aus

Wenn Schadsoftware entdeckt wird, kann Kaspersky Endpoint Security die infizierte Datei löschen und den von dieser Datei gestarteten schädlichen Prozess beenden. In den Einstellungen für Schutz vor bedrohlichen Dateien können Sie die Aktion auswählen, die Kaspersky Endpoint Security beim Erkennen einer Bedrohung ausführt.

So konfigurieren Sie die Aktion beim Erkennen einer Bedrohung in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Schutz vor bedrohlichen Dateien**.
5. Wählen Sie unter **Aktion beim Fund einer Bedrohung** die Aktion aus, die das Programm ausführen soll, wenn eine Bedrohung erkannt wird:

   - **Desinfizieren – Löschen, wenn Desinfektion fehlschlägt** (Standardeinstellung). Wenn diese Option ausgewählt ist, versucht das Programm automatisch, die gefundene infizierte Datei zu desinfizieren. Wenn die Desinfektion nicht möglich ist, wird die Datei vom Programm gelöscht.
   - **Desinfizieren – Blockieren, wenn Desinfektion fehlschlägt**. Wenn diese Option ausgewählt ist, versucht das Programm automatisch, die gefundene infizierte Datei zu desinfizieren. Wenn die Desinfektion fehlschlägt, wird die Datei durch die Anwendung blockiert.
   - **Blockieren**. Wenn diese Option ausgewählt ist, wird die infizierte Datei automatisch durch die Anwendung blockiert und es erfolgt kein Desinfektionsversuch.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie die Aktion beim Erkennen einer Bedrohung über die Befehlszeile

1. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control --set-settings 1 ActionOnThreat=<DisinfectDeleteIfNotPossible|DisinfectBlockIfNotPossible|Block>
   ```
2. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --get-settings 1
   ```

Symbole

Befehlsoptionen

Parameter	Description
`ActionOnThreat`	Aktion beim Erkennen einer Bedrohung: • `DisinfectDeleteIfNotPossible` (Standardeinstellung). Wenn diese Option ausgewählt ist, versucht das Programm automatisch, die gefundene infizierte Datei zu desinfizieren. Wenn die Desinfektion nicht möglich ist, wird die Datei vom Programm gelöscht. • `DisinfectBlockIfNotPossible`. Wenn diese Option ausgewählt ist, versucht das Programm automatisch, die gefundene infizierte Datei zu desinfizieren. Wenn die Desinfektion fehlschlägt, wird die Datei durch die Anwendung blockiert. • `Block`. Wenn diese Option ausgewählt ist, wird die infizierte Datei automatisch durch die Anwendung blockiert und es erfolgt kein Desinfektionsversuch.

Was ist der intelligente Modus der Dateiuntersuchung?

Der Schutz vor bedrohlichen Dateien untersucht alle Dateien, die geöffnet, gespeichert oder ausgeführt werden. Standardmäßig untersucht der Schutz vor bedrohlichen Dateien Dateien im intelligenten Modus. Im *intelligenten Modus* untersucht der Schutz vor bedrohlichen Dateien eine Datei, wenn versucht wird, sie zu öffnen. Wenn ein Prozess über einen bestimmten Zeitraum wiederholt auf eine Datei zugreift und sie ändert, untersucht der Schutz vor bedrohlichen Dateien die Datei erst dann erneut, wenn dieser Prozess sie schließt. Dadurch werden die Auswirkungen des Programms auf die Systemleistung minimiert und gleichzeitig ein hohes Maß an Schutz bereitgestellt.

Damit der intelligente Modus funktioniert, muss das aktualisierbare Kernel-Modul ausgewählt und gestartet werden.

Der Untersuchungsmodus für Dateien kann in der Web Console nicht geändert werden.

So wählen Sie den Untersuchungsmodus für Dateien über die Befehlszeile aus

1. Führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 1 ScanByAccessType=<SmartCheck|OpenAndModify|Open>
```

2. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 1
```

Symbole

Befehlsoptionen

Parameter	Description
`ScanByAccessType`	Untersuchungsmodus für Dateien: • `SmartCheck` (Standardwert). Der Schutz vor bedrohlichen Dateien untersucht Dateien im intelligenten Modus. Kaspersky Endpoint Security untersucht eine Datei beim Öffnen und beim Schließen, wenn die Datei geändert wurde. Wenn der intelligente Modus nicht verfügbar ist, untersucht das Programm Dateien, wenn sie geöffnet werden und jedes Mal, wenn die Datei geändert wird (`OpenAndModify`). Der intelligente Modus ist beispielsweise möglicherweise nicht verfügbar, wenn das aktualisierbare Kernel-Modul angehalten ist. • `OpenAndModify`. Kaspersky Endpoint Security untersucht eine Datei beim Öffnen und bei jeder Änderung der Datei, nicht nur beim Schließen. • `Open`. Kaspersky Endpoint Security untersucht eine Datei, wenn versucht wird, sie zum Lesen, Ausführen oder Ändern zu öffnen.

So optimieren Sie die Untersuchung von Dateien

Konfigurieren Sie die Untersuchung von Dateien, um die Komponente „Schutz vor bedrohlichen Dateien“ zu optimieren. Dadurch wird die CPU-Auslastung auf dem geschützten Gerät reduziert. Sie können die Untersuchung von Archiven einschränken, die maximale Größe der Objekte festlegen, die untersucht werden können, und die maximale Dauer der Objektuntersuchung festlegen.

So konfigurieren Sie die Untersuchung von Dateien über die Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Schutz vor bedrohlichen Dateien**.
5. Wählen Sie unter **Erweiterte Einstellungen** die Registerkarte **Leistung** aus und konfigurieren Sie die Untersuchung von Dateien:

   - **Archive untersuchen**. Untersucht Archive der Formate ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE und mehr. Die Anwendung durchsucht Archive nicht nur nach Dateiendung, sondern auch nach Format. Bei der Untersuchung von Archiven entpackt die Anwendung diese rekursiv. Dadurch können Bedrohungen in verschachtelten Archiven (d. h. Archive in Archiven) erkannt werden. Die Untersuchung ist standardmäßig deaktiviert.
   - **Programmpakete und selbstextrahierende Archive untersuchen**. Untersuchung von Installationspaketen für Drittanbieter-Anwendungen und von selbstextrahierenden Archiven. Selbstentpackende Archive sind Archive, die ein ausführbares Modul zum Entpacken enthalten. Die Untersuchung ist standardmäßig deaktiviert.
   - **E-Mail-Datenbanken untersuchen**. Untersuchung von E-Mail-Datenbanken für Microsoft Outlook, Outlook Express, The Bat! und andere E-Mail-Programme. Die Untersuchung ist standardmäßig deaktiviert.
   - **Dateien in E-Mail-Formaten untersuchen**. E-Mail-Nachrichten im Nur-Text-Format untersuchen. Die Untersuchung ist standardmäßig deaktiviert.
   - **Archive nicht untersuchen, wenn größer als (MB)**. Maximale Größe des zu untersuchenden Objekts (in Megabyte). Wenn die Größe des zu untersuchenden Objekts den angegebenen Wert überschreitet, überspringt die Anwendung das Objekt während der Untersuchung.
   - **Datei überspringen, wenn Untersuchung länger dauert als (Sek.)**. Maximale Untersuchungsdauer (in Sekunden) eines Objekts. Die Anwendung stellt die Untersuchung eines Objekts ein, wenn sie länger dauert als durch diese Einstellung festgelegt. Standardmäßig versucht das Programm, ein Objekt innerhalb einer Minute zu untersuchen.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie die Untersuchung von Dateien über die Befehlszeile

1. Führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 1 ScanArchived=<Yes|No> ScanSfxArchived=<Yes|No> ScanMailBases=<Yes|No>
ScanPlainMail=<Yes|No> SkipPlainTextFiles=<Yes|No> SkipDatabaseJournals=<Yes|No> SizeLimit=<Object size (MB)>
TimeLimit=<Scan time (sec)>
```

2. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 1
```

Symbole

Befehlsoptionen

Parameter	Description
`ScanArchived`	Untersucht Archive der Formate ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE und mehr. Die Anwendung durchsucht Archive nicht nur nach Dateiendung, sondern auch nach Format. Bei der Untersuchung von Archiven entpackt die Anwendung diese rekursiv. Dadurch können Bedrohungen in verschachtelten Archiven (d. h. Archive in Archiven) erkannt werden. Die Untersuchung ist standardmäßig deaktiviert.
`ScanSfxArchived`	Untersuchung von Installationspaketen für Drittanbieter-Anwendungen und von selbstextrahierenden Archiven. Selbstentpackende Archive sind Archive, die ein ausführbares Modul zum Entpacken enthalten. Die Untersuchung ist standardmäßig deaktiviert.
`ScanMailBases`	Untersuchung von E-Mail-Datenbanken für Microsoft Outlook, Outlook Express, The Bat! und andere E-Mail-Programme. Die Untersuchung ist standardmäßig deaktiviert.
`ScanPlainMail`	E-Mail-Nachrichten im Nur-Text-Format untersuchen. Die Untersuchung ist standardmäßig deaktiviert.
`SkipPlainTextFiles`	Dateien im Textformat vorübergehend von der Untersuchung ausschließen. Das Programm untersucht Textdateien nicht, wenn sie vom selben Prozess innerhalb von 10 Minuten nach der letzten Untersuchung wiederverwendet werden. Die Ausnahme von der Untersuchung ist standardmäßig deaktiviert. Diese Einstellung ist für Geräte vorgesehen, die den fanotify-Mechanismus zum Abfangen von Systemereignissen unterstützen. Auf Geräten mit dem aktualisierbaren Kernel-Modul verwendet das Programm den Cache für Untersuchungsergebnisse, um die Auslastung zu optimieren.
`SkipDatabaseJournals`	Schließt Protokolldateien von Datenbanken vorübergehend von der Untersuchung aus. Das Programm untersucht Datenbank-Journaldateien nicht, wenn die Journaldatei vom selben Prozess innerhalb von 10 Minuten nach der letzten Untersuchung wiederverwendet wird. Die Ausnahme von der Untersuchung ist standardmäßig deaktiviert. Diese Einstellung ist für Geräte vorgesehen, die den fanotify-Mechanismus zum Abfangen von Systemereignissen unterstützen. Auf Geräten mit dem aktualisierbaren Kernel-Modul verwendet das Programm den Cache für Untersuchungsergebnisse, um die Auslastung zu optimieren.
`SizeLimit`	Maximale Größe des zu untersuchenden Objekts (in Megabyte). Wenn die Größe des zu untersuchenden Objekts den angegebenen Wert überschreitet, überspringt die Anwendung das Objekt während der Untersuchung. (Wert `0`).
`TimeLimit`	Maximale Untersuchungsdauer (in Sekunden) eines Objekts. Die Anwendung stellt die Untersuchung eines Objekts ein, wenn sie länger dauert als durch diese Einstellung festgelegt. Standardmäßig versucht das Programm, ein Objekt innerhalb einer Minute zu untersuchen. (Wert `60`).

Besonderheiten der Untersuchung von symbolischen Links und festen Links

Kaspersky Endpoint Security ermöglicht die Untersuchung symbolischer und fester Links zu Dateien.

Ein *symbolischer Link* (auch als Soft link bezeichnet) ist eine Datei, die auf eine andere Datei oder ein anderes Verzeichnis verweist. Ein symbolischer Link und die Datei, auf die er verweist, können sich in verschiedenen Dateisystemen befinden. Außerdem kann ein solcher Link auf eine Datei verweisen, die nicht vorhanden ist. Wenn Sie die Zieldatei löschen, wird der Link nicht gelöscht, aber er funktioniert nicht mehr.

Ein *Hard link* ist im Wesentlichen ein alternativer Name für die Datei. Ein fester Link verweist auf den Indexdeskriptor (Inode) der Datei, der die Metadaten der Datei enthält. Solange mindestens ein fester Link zu der Datei vorhanden ist, bleibt die Datei im Dateisystem bestehen.

Untersuchung von symbolischen Links

Die App untersucht symbolische Links nur dann, wenn die Datei, auf die der symbolische Link verweist, im Schutzbereich des Schutzes vor bedrohlichen Dateien liegt.

Wenn sich die Datei außerhalb des Schutzbereichs befindet, folgt die App dem symbolischen Link nicht, um den Inhalt der Datei zu untersuchen. Sollte die Datei jedoch bösartigen Code enthalten, ist die Sicherheit des Geräts gefährdet.

Untersuchung von festen Links

Wenn in einer Datei, auf die mehr als ein fester Link verweist, schädlicher Code gefunden wird, desinfiziert die App die Originaldatei. Wenn eine Desinfektion nicht möglich ist, löscht die App den festen Link und erstellt an seiner Stelle eine Kopie der Quelldatei mit dem Namen des gelöschten Links im Backup. Die App löscht nur den festen Link, der gerade verarbeitet wird; die übrigen festen Links, die möglicherweise auf dieselben Daten verweisen, bleiben intakt.

Wenn Sie einen festen Link aus dem Backup wiederherstellen, erstellt die App am ursprünglichen Speicherort eine Kopie der Originaldatei mit dem Namen des wiederherzustellenden festen Links. Der wiederhergestellte Link wird nicht zu einem festen Link auf die Originaldatei und bleibt von den anderen festen Links auf dieselbe Datei unabhängig.

Auflösen symbolischer Links in prozessbezogenen Ausnahmen

Wenn der Pfad im Parameter `ProgramPath` des Abschnitts `ExcludedForProgram` ein symbolischer Link zu einer ausführbaren Binärdatei ist, wendet das Programm die Ausnahme auf den Pfad der Zieldatei an. Diese Regel gilt für alle Links zu dieser Datei und nicht nur für den explizit angegebenen Link. Dieser Parameter verwendet den Pfad zum Programmabbild. Daher werden symbolische Links zu Skripten (z. B. `.sh`) nicht aufgelöst.

Die Zieldatei wird beim Ausführen der Aufgabe und beim Übernehmen der Einstellungen ermittelt. Wenn ein Link auf eine nicht vorhandene Datei verweist, wird der Pfad zum Link selbst in die Ausnahmen aufgenommen. Wenn der Link durch eine reguläre ausführbare Datei mit demselben Namen ersetzt wird, wird die Ausnahme auf diese Datei angewendet.

Beispiel für eine Ausnahme mit einem symbolischen Link

```
[ExcludedForProgram.item_0000]
ProgramPath=/usr/bin/md5sum
UseExcludedForProgram=Yes
Path=/root/s1
```

Beim Start der Aufgabe verweist der Link `/usr/bin/md5sum` auf `/bin/coreutils`, sodass `/bin/coreutils` zu den Ausnahmen hinzugefügt wird. Wenn der Link später auf `/bin/false` umgeleitet wird, bleibt die Ausnahme bis zum Neustart der Aufgabe für `/bin/coreutils` bestehen und wird nicht auf `/bin/false` angewendet. Nach dem Neustart der Aufgabe wird die Ausnahme auf `/bin/false` statt auf `/bin/coreutils` angewendet.

Schadsoftware-Untersuchung.

Die Schadsoftware-Untersuchung ist ein wichtiger Faktor für die Gewährleistung der Computersicherheit. Schadsoftware-Untersuchungen sollten regelmäßig durchgeführt werden, um eine mögliche Ausbreitung von schädlichen Programmen auszuschließen, die von den Schutzkomponenten beispielsweise aufgrund einer zu niedrigen Schutzstufe nicht erkannt wurden.

In Kaspersky Endpoint Security ist die Standardaufgabe *Schadsoftware-Untersuchung* vordefiniert. Mit dieser Aufgabe können Sie eine vollständige Untersuchung des Geräts durchführen. Bei der vollständigen Untersuchung untersucht die Anwendung 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.

Der Assistent für die Ersteinrichtung des Administrationsservers erstellt automatisch eine Aufgabe *Schadsoftware-Untersuchung*. Um eine Aufgabe *Schadsoftware-Untersuchung* zu erstellen, installieren Sie während der Ausführung des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Linux. Bei Bedarf können Sie Benutzeraufgaben vom Typ *Schadsoftware-Untersuchung* erstellen.

Einstellungen der Aufgabe Schadsoftware-Untersuchung

1. **Ausführungszeitplan der Aufgabe konfigurieren**

   Während der Untersuchung kann Kaspersky Endpoint Security mehr Computerressourcen als gewöhnlich beanspruchen. Wir empfehlen, Untersuchungsaufgaben für Zeiten zu planen, in denen der Computer am wenigsten ausgelastet ist.

2. **Systembelastung durch die Untersuchung optimieren**

   Sie können beim Ausführen der Aufgabe „Schadsoftware-Untersuchung“ die CPU-Auslastung beschränken. Dadurch kann die Untersuchung Ihres Computers länger dauern.

   Kaspersky Endpoint Security ermöglicht das Abbrechen geplanter Aufgaben, wenn ein Laptop im Akkubetrieb läuft.

3. **Einstellungen der Aufgabe „Schadsoftware-Untersuchung“ konfigurieren**

   Standardmäßig verwendet die Aufgabe „Schadsoftware-Untersuchung“ die von Kaspersky-Experten empfohlenen Einstellungen. Die Standardeinstellungen bieten das empfohlene Schutzniveau und eine optimale Ressourcennutzung. Wenn Sie spezielle Anforderungen an die Sicherheit der Infrastruktur haben, können Sie diese Einstellungen ändern.

   Standardmäßig untersucht das Programm Archive. Dazu entpackt das Programm die Archive in das Verzeichnis /tmp. Stellen Sie sicher, dass auf dem Computer genügend freier Speicherplatz zum Entpacken der Archive vorhanden ist.

4 Untersuchungsbereich konfigurieren

Standardmäßig untersucht das Programm alle Dateien auf einem geschützten Gerät. Wenn Sie nur ein einzelnes Verzeichnis untersuchen müssen (z. B. das Verzeichnis, in das Dateien automatisch aus einer externen Quelle heruntergeladen werden), können Sie nur dieses Verzeichnis als Untersuchungsbereich angeben. In anderen Fällen empfehlen wir, den standardmäßigen Untersuchungsbereich beizubehalten und den Bereich mithilfe von Ausnahmen genauer anzupassen.

> Zum Untersuchen von Servern empfehlen wir, den Untersuchungsbereich in mehrere Teilbereiche aufzuteilen und für jeden dieser Teilbereiche eine separate Aufgabe „Schadsoftware-Untersuchung“ zu erstellen. Um die Last zu verteilen, planen Sie für jede Aufgabe eine andere Startzeit ein.

5 Untersuchungsausnahmen hinzufügen

Richten Sie einen Ausnahmebereich ein:

- **Untersuchungsausnahmen**. Ausnahmen helfen dabei, Systemsicherheit und Leistung in Einklang zu bringen. Für einen stabilen Betrieb von Drittanbieter-Software fügen Sie den Ausnahmen die Dateien und Verzeichnisse hinzu, die in der Dokumentation der jeweiligen Software aufgeführt sind.

  Wenn Sie bereits einen Ausnahmebereich für die Komponente Schutz vor bedrohlichen Dateien erstellt haben, können Sie diese Ausnahmen auch auf die Aufgabe „Schadsoftware-Untersuchung“ anwenden.

- **Globale Ausnahmen**. Wenn Sie Mount-Punkte ausschließen (globale Ausnahmen), fängt das Programm Dateivorgänge in bestimmten Verzeichnissen nicht ab. Schließen Sie freigegebene Netzwerkressourcen aus dem Untersuchungsbereich aus. Um gemeinsam genutzte Netzwerkressourcen zu schützen, können Sie Kaspersky Endpoint Security direkt auf dem Gerät verwenden, welches die Ressourcen physisch speichert.

6 Aufgabe „Schadsoftware-Untersuchung“ starten

So starten Sie die Aufgabe zur Schadsoftware-Untersuchung in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe *Schadsoftware-Untersuchung*.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Die Aufgabe *Schadsoftware-Untersuchung* wird automatisch vom Schnellstartassistenten des Administrationsservers erstellt. Um eine Aufgabe *Schadsoftware-Untersuchung* zu erstellen, installieren Sie während der Ausführung des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Linux.

   Bei Bedarf können Sie Benutzeraufgaben vom Typ *Schadsoftware-Untersuchung* erstellen.

3. Verwalten Sie auf der Registerkarte **Einstellungen** die Aufgabeneinstellungen.

4. Konfigurieren Sie auf der Registerkarte **Anwendungseinstellungen** die erweiterten Einstellungen des Programms (siehe Tabelle unten).

5. Konfigurieren Sie auf der Registerkarte **Zeitplan**, wie die Aufgabe gestartet werden soll.

   Kaspersky Endpoint Security ist standardmäßig so konfiguriert, dass die Aufgabe manuell ausgeführt wird.

6. Speichern Sie die vorgenommenen Änderungen.

7. Führen Sie die Aufgabe aus.

Einstellungen der Aufgabe *Schadsoftware-Untersuchung*

Einstellung	Description
Untersuchungsbereich	Eine Tabelle mit Bereichen, die von der Aufgabe untersucht werden sollen. Standardmäßig ist nur ein Untersuchungsbereich aktiv; dieser umfasst alle Verzeichnisse des lokalen Dateisystems. Sie können Untersuchungsbereiche manuell hinzufügen.
Aktion beim Fund einer Bedrohung	• **Desinfizieren – Löschen, wenn Desinfektion fehlschlägt** (Standardwert). Wenn Sie diese Aktion auswählen, versucht die Anwendung, das infizierte Objekt zu desinfizieren, indem sie eine Kopie des Objekts im Backup-Speicher speichert. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), löscht die Anwendung das Objekt. • **Desinfizieren – Informieren, wenn Desinfektion fehlschlägt**. Wenn Sie diese Aktion auswählen, versucht die Anwendung, das infizierte Objekt zu desinfizieren, indem sie eine Kopie des Objekts im Backup-Speicher speichert. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), speichert die Anwendung Informationen darüber im Protokoll. • **Informieren**. Wenn Sie diese Aktion auswählen, speichert die Anwendung Informationen über das infizierte Objekt im Protokoll.
Archive untersuchen	Wenn diese Option aktiviert ist, untersucht das Programm Archive. Die Anwendung 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. Um ein Archiv zu untersuchen, muss es zunächst von der Anwendung entpackt werden, was die Untersuchung verlangsamen kann. Sie können die Dauer der Untersuchung von Archiven verkürzen, indem Sie die Einstellungen **Datei überspringen, wenn Untersuchung länger dauert als (Sek.)** und **Dateien nicht untersuchen, wenn größer als (MB)** festlegen. Diese Option ist standardmäßig deaktiviert.
Programmpakete und selbstextrahierende Archive untersuchen	Wenn diese Option aktiviert ist, untersucht das Programm selbstentpackende Archive. Selbstentpackende Archive sind Archive, die ein ausführbares Modul zum Entpacken enthalten. Diese Option ist standardmäßig deaktiviert.
Dateien in E-Mail-Formaten untersuchen	Wenn diese Option aktiviert ist, untersucht das Programm E-Mail-Nachrichten im Textformat. Die Funktion ist standardmäßig deaktiviert.
E-Mail-Datenbanken untersuchen	Wenn diese Option aktiviert ist, untersucht das Programm Mail-Datenbanken von Microsoft Outlook, Outlook Express, The Bat! und anderen Mail-Anwendungen. Die Funktion ist standardmäßig deaktiviert.
Dateien nicht untersuchen, wenn größer als (MB)	Sie können die maximale Größe einer Datei, die untersucht werden kann, in Megabyte angeben. Zulässige Werte: 1 – 999999. Diese Einschränkung ist standardmäßig deaktiviert.
Datei überspringen, wenn Untersuchung länger dauert als (Sek.)	Sie können die maximale Untersuchungsdauer für eine Datei in Sekunden angeben. Nach Ablauf des angegebenen Zeitraums bricht die Anwendung die Untersuchung der Datei ab. Zulässige Werte: 1 – 9999. Diese Einschränkung ist standardmäßig deaktiviert.
Nicht mehrere Untersuchungsaufgaben gleichzeitig ausführen	Aufgeschobener Start von Untersuchungsaufgaben, wenn bereits eine Untersuchungsaufgabe ausgeführt wird. Kaspersky Endpoint Security reiht neue Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Beispiel: Das Programm hat nach Zeitplan eine vollständige Untersuchungsaufgabe gestartet. Wenn ein Benutzer versucht, eine schnelle Untersuchung über die Programmoberfläche zu starten, stellt Kaspersky Endpoint Security diese Aufgabe zur schnellen Untersuchung in die Warteschlange und startet diese Aufgabe automatisch, nachdem die vollständige Untersuchungsaufgabe abgeschlossen wurde. Die Funktion ist standardmäßig deaktiviert.
iChecker-Technologie verwenden	Wenn diese Option aktiviert ist, untersucht das Programm nur neue Dateien sowie Dateien, die nach der letzten Untersuchung geändert wurden. Wenn diese Option deaktiviert ist, untersucht das Programm Dateien unabhängig von ihrem Erstellungs- oder Änderungsdatum. Diese Option ist standardmäßig deaktiviert.

So starten Sie die Aufgabe „Schadsoftware-Untersuchung“ über die Befehlszeile

1. Standardmäßig verfügt die Anwendung über die Aufgabe *Schadsoftware-Untersuchung* (*Scan_My_Computer*). Wenn Sie eine neue Aufgabe *Schadsoftware-Untersuchung* erstellen möchten, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --create-task <task name> --type ODS
   ```

   wobei `<task name>` der Name ist, den Sie für die neue Aufgabe festlegen möchten.

   Dieser Befehl gibt die ID der erstellten Aufgabe zurück.

2. Bei Bedarf können Sie die Aufgabeneinstellungen ändern (siehe Tabelle unten), indem Sie den folgenden Befehl verwenden:

   ```
   kesl-control --set-settings <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

   Beispiel für das Ändern der Aufgabeneinstellungen

   ```
   kesl-control --set-settings 101 ScanFiles=No
   ```

   Sie können die Aufgabeneinstellungen auch mithilfe einer Konfigurationsdatei verwalten.

3. Konfigurieren Sie bei Bedarf einen Zeitplan für die Aufgabe. Standardmäßig wird die Aufgabe manuell gestartet.

4. Um die aktuellen Werte der Aufgabeneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --get-settings <task ID|name>
   ```

5. Um die Aufgabe *Schadsoftware-Untersuchung* zu starten, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --start-task <task ID|name> [-W] [--progress]
   ```

   Befehlsbeispiele

   ```
   kesl-control --start-task 2 -W
   ```

6. Um die Aufgabe *Schadsoftware-Untersuchung* zu beenden, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --stop-task <task ID|name> [-W]
   ```

Symbole

Einstellungen der Aufgabe Schadsoftware-Untersuchung

Einstellung	Description	Werte
`ScanFiles`	Aktiviert die Untersuchung von Dateien.	`Yes` (Standardwert) – Dateien untersuchen. `No` – Dateien nicht untersuchen.
`ScanBootSectors`	Aktiviert die Untersuchung der Bootsektoren.	`Yes` (Standardwert) – Bootsektoren untersuchen. `No` – Bootsektoren nicht untersuchen.

Einstellung	Description	Werte
`ScanComputerMemory`	Aktiviert die Untersuchung des Prozess- und Kernelspeichers.	`Yes` (Standardwert) – Prozessspeicher und Kernelspeicher untersuchen. `No` – Prozessspeicher und Kernelspeicher nicht untersuchen.
`ScanStartupObjects`	Aktiviert die Untersuchung der Autostart-Objekte.	`Yes` (Standardwert) – Autostart-Objekte untersuchen. `No` – Autostart-Objekte nicht untersuchen.
`ScanArchived`	Aktiviert die Untersuchung von Archiven (einschließlich selbstentpackender sfx-Archive). Die Anwendung 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 untersuchen. Wenn für den Parameter `ActionOnThreat` der Wert `DisinfectDeleteIfNotPossible` angegeben und eine Desinfizierung nicht möglich ist, löscht die Anwendung je nach Archivtyp entweder das infizierte Objekt oder das gesamte Archiv, das die Bedrohung enthält. `No` – Archive nicht untersuchen.
`ScanSfxArchived`	Aktiviert die Untersuchung ausschließlich von self-extracting archives (Archiven, die ein ausführbares Entpackmodul enthalten).	`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 Format plain text.	`Yes` – E-Mail-Nachrichten im Nur-Text-Format untersuchen. `No` (Standardwert) – E-Mail-Nachrichten im 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.
`QueueScanTasks`	Geplante Untersuchungsaufgaben verzögern, wenn eine zuvor gestartete geplante Untersuchung noch ausgeführt wird. Kaspersky Endpoint Security reiht geplante Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Eine Untersuchungsaufgabe soll beispielsweise um 18:00 Uhr und um 20:00 Uhr ausgeführt werden. Die für 20:00 Uhr geplante Untersuchungsaufgabe wird verzögert, wenn die Untersuchung um 18:00 Uhr noch ausgeführt wird. Die verzögerte Aufgabe wird ausgeführt, nachdem die Aufgabe um 18:00 Uhr beendet wurde.	`Yes`, um geplante Untersuchungsaufgaben in die Warteschlange einzureihen, wenn die aktuelle Untersuchung noch ausgeführt wird. `No` (Standardwert), um geplante Untersuchungsaufgaben auch dann auszuführen, wenn die aktuelle Untersuchung noch ausgeführt wird.

Einstellung	Description	Werte
`ActionOnThreat`	Auswahl der Aktion, welche die Anwendung für infizierte Objekte ausführen soll.	`DisinfectDeleteIfNotPossible` (Desinfizieren. Entfernen, wenn Desinfektion fehlschlägt) – Die Anwendung versucht, das infizierte Objekt zu desinfizieren und speichert eine Kopie des Objekts im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), löscht die Anwendung das Objekt. `DisinfectInformIfNotPossible` (Desinfizieren. Informieren, wenn Desinfektion fehlschlägt) – Die Anwendung versucht, das infizierte Objekt zu desinfizieren und speichert eine Kopie des Objekts im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), speichert die Anwendung Informationen darüber im Protokoll. `Inform` (Informieren) – Die Anwendung unternimmt keinen Versuch, das infizierte Objekt zu desinfizieren oder zu löschen. Informationen über das infizierte Objekt werden im Protokoll gespeichert. Der Standardwert ist: `DisinfectDeleteIfNotPossible`.
`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, von Untersuchungen ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht von der Untersuchung ausschließen.

`ExcludeMasks.item_#`	Ausnahme 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 die Werte 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, aus der Untersuchung.	`Yes` – Objekte, welche die in der Einstellung `ExcludeThreats.item_#` angegebenen Bedrohungen enthalten, von der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die Bedrohungen enthalten, die in der Einstellung `ExcludeThreats.item_#` angegeben sind, nicht von der Untersuchung ausschließen.

Einstellung	Description	Werte

`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 verwenden, um Informationen über Ihr Netzwerk zu erhalten. 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 Anwendung 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` – Globale Ausnahmen nicht verwenden.
`UseOASExclusions`	Aktivieren der Verwendung der Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der Untersuchung.	`Yes` (Standardwert) – Ausschlüsse aus dem Schutz vor bedrohlichen Dateien verwenden. `No` – Ausnahmen für den Schutz vor bedrohlichen Dateien nicht 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 untersuchte Objekte in Archiven 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. 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.

Einstellung	Description	Werte
`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 mit minimaler Belastung des Systems. `Medium` – Eine mittlere Stufe der heuristischen Analyse bei ausgewogener Systemauslastung. `Deep` – Die gründlichste Untersuchung bei maximaler Systemauslastung. `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 Gerätenamen. Die App untersucht die Bootsektoren dieser Geräte. Der Einstellungswert darf nicht leer sein. Um die Aufgabe auszuführen, müssen Sie mindestens eine Maske für Gerätenamen angeben.	`AllObjects` – Untersuchung der Bootsektoren aller Geräte. `<device name mask>` – Bootsektoren der Geräte untersuchen, deren Namen der angegebenen Maske entsprechen. Standardwert: `/**` (beliebiger Zeichensatz im Gerätenamen, einschließlich des Zeichens `/`)
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.	Der Standardwert ist: `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 Anwendung 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_0000=*doc`

Einstellung	Description	Werte
`Path`	Pfad zum Verzeichnis mit untersuchten Objekten.	`<path to local directory>` – Objekte in dem angegebenen Verzeichnis untersuchen. Standardmäßige Pfadangabe `/` – Die Anwendung untersucht alle Verzeichnisse des lokalen Dateisystems. `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. `<file system type>` – Alle Ressourcen des angegebenen Dateisystemgeräts 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 Anwendung 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 ausschließen)

Einstellung	Description	Werte
`Path`	Pfad zum Verzeichnis mit ausgeschlossenen Objekten.	`<path to local directory>` – Objekte im angegebenen Verzeichnis (einschließlich Unterverzeichnissen) von Untersuchungen ausschließen. Bei der Angabe des Pfades können Masken verwendet werden. 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/`. Der Pfad `/` ist standardmäßig angegeben. Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus. `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. `<file system type>` – Alle Ressourcen des angegebenen Dateisystemgeräts von der Untersuchung ausschließen. Remote-Verzeichnisse werden nur dann von der Untersuchung durch die Anwendung ausgeschlossen, wenn sie bereits vor dem Aufgabenstart eingebunden wurden. Remote-Verzeichnisse, die erst nach dem Aufgabenstart eingebunden wurden, werden von der Untersuchung nicht ausgeschlossen.

So führen Sie die Aufgabe zur Schadsoftware-Untersuchung über die grafische Benutzeroberfläche aus

1. Öffnen Sie das Hauptfenster der grafischen Benutzeroberfläche des Programms.
2. Klicken Sie auf die Schaltfläche **Untersuchung**.

   Das Fenster **Untersuchung** wird geöffnet.
3. Um eine Untersuchungsaufgabe zu starten, klicken Sie unter der Untersuchungsaufgabe, die Sie starten möchten, auf die Schaltfläche **Starten**.

   Der Fortschritt der laufenden Untersuchungsaufgabe wird angezeigt.
4. Um eine Untersuchungsaufgabe anzuhalten, klicken Sie unter der Untersuchungsaufgabe, die Sie anhalten möchten, auf die Schaltfläche **Stoppen**.

   Die Untersuchungsaufgabe wird angehalten und es werden Informationen zu untersuchten Objekten und erkannten Bedrohungen angezeigt.
5. Um den Bericht zur Untersuchungsaufgabe anzuzeigen, klicken Sie auf die Schaltfläche **Bericht anzeigen**.

Wenn ein infiziertes Objekt gefunden wird oder eine Untersuchungsaufgabe abgeschlossen ist, wird eine entsprechende Benachrichtigung angezeigt.

Das Fenster **Untersuchung** zeigt außerdem 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}*) an.

7 Statistiken zur Computer-Untersuchung sammeln

Mithilfe von Berichten können Sie Untersuchungsstatistiken für einen Computer abrufen. Stellen Sie sicher, dass die Untersuchungsdauer innerhalb des zulässigen Bereichs liegt. Überprüfen Sie die gefundenen Objekte und fügen Sie sie zu den Ausnahmen hinzu, wenn diese Objekte vertrauenswürdig sind.

Besonderheiten und Einschränkungen

- Wenn der Root-Benutzer keinen Zugriff auf ein Remote-Verzeichnis hat, das auf dem Gerät über das NFSv4-Protokoll eingebunden ist, überspringt das Programm diese Datei während der Untersuchung.
- 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 nicht gespeichert.
- Wenn der Benutzer oder der Watchdog-Dienst die Anwendung während der Schadsoftware-Untersuchung neu startet oder wenn der Computer während der Untersuchung neu gestartet wird, wird die Untersuchung gestoppt. Beim nächsten Start der Schadsoftware-Untersuchung beginnt sie von vorne.

Nützliche Artikel

Vorgehensweise, wenn auf Ihrem Gerät kein freier Speicherplatz mehr verfügbar ist

So erstellen Sie einen Untersuchungsbereich

Ein *Untersuchungsbereich* ist eine Liste von Pfaden zu Objekten, die Kaspersky Endpoint Security auf Bedrohungen untersucht. Standardmäßig untersucht das Programm alle Dateien auf einem geschützten Gerät. Wenn Sie nur ein einzelnes Verzeichnis untersuchen müssen (z. B. das Verzeichnis, in das Dateien automatisch aus einer externen Quelle heruntergeladen werden), können Sie dieses Verzeichnis als Untersuchungsbereich angeben.

Kaspersky Endpoint Security untersucht Objekte in der Reihenfolge, in der sie in der Liste der Objekte aufgeführt 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.

Bei Betriebssystemen mit speziellem parsecfs-Dateisystem (Astra Linux Special Edition) wird es empfohlen, die Mount-Pfade dieses Dateisystems zu den Untersuchungsausnahmen hinzuzufügen.

So erstellen Sie einen Untersuchungsbereich in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Untersuchungsaufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Klicken Sie im Abschnitt **Untersuchungsbereich** auf **Hinzufügen**.

5. Wählen Sie in der Dropdown-Liste **Dateisystem, Zugriffsprotokoll und Pfad** den Typ des Dateisystems aus:

   - **Lokal**. Verzeichnisse auf der Festplatte, auf die ohne Netzwerkverbindung zugegriffen werden kann.
   - **Eingehängt**. Eingebundene Remote- oder lokale Verzeichnisse.
   - **Freigegeben**. Computerverzeichnisse, auf die über das Samba- (SMB) oder das NFS-Protokoll zugegriffen werden kann.
   - **Alle remote eingehängten**. Alle Remote-Verzeichnisse, die auf dem Gerät über die Protokolle Samba und NFS eingebunden sind.
   - **Alle freigegebenen**. Alle Computerverzeichnisse, auf die über die Protokolle Samba und NFS zugegriffen wird.

6. Wählen Sie für die Dateisystemtypen **Eingehängt** und **Freigegeben** ein Zugriffsprotokoll aus:

   - **NFS**. Remote-Verzeichnisse, die auf einem Gerät über das NFS-Protokoll eingebunden sind.
   - **Samba**. Remote-Verzeichnisse, die auf einem Gerät über das Samba-Protokoll eingebunden sind.
   - **Benutzerdefiniert** Dateisystemressourcen auf einem Gerät mit einem anderen Typ als NFS oder Samba (z. B. `ext4` oder `parsecfs`).

7. Geben Sie den Pfad zum Verzeichnis oder eine Pfadmaske an.

8. Geben Sie bei Bedarf Masken für Objektnamen an (z. B. `*.txt` oder `report_*`). Trennen Sie die Masken durch Kommas.

9. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das neue Objekt wird dem Untersuchungsbereich hinzugefügt. Sie können ein Objekt aus dem Untersuchungsbereich ausschließen, ohne es aus der Liste der Objekte zu entfernen. Deaktivieren Sie dazu den Umschalter neben dem Objekt.

10. Aktivieren oder deaktivieren Sie bei Bedarf die vordefinierten Objekte im Untersuchungsbereich:

    - **Kernel-Speicher**. **Speicher für aktive Prozesse**.
    - **Aktive Prozesse und Autostart-Objekte**.
    - **Laufwerksbootsektoren**.
    - **Alle Festplatten**.
    - **Alle Netzlaufwerke**.

11. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So erstellen Sie einen Untersuchungsbereich über die Befehlszeile

1. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control --set-settings 2 --add-path <path>
   ```

   Den Aufgabeneinstellungen wird ein neuer Abschnitt vom Typ `[ScanScope.item_#]` hinzugefügt. Die App untersucht die Objekte im angegebenen Verzeichnis.

   Beispiel

   ```
   kesl-control --set-settings 2 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
   ```

   Die folgenden Einstellungen für den Untersuchungsbereich werden der Aufgabe hinzugefügt:

   ```
   [ScanScope.item_0001]
   AreaDesc=All objects
   UseScanArea=Yes
   Path=/home
   AreaMask.item_0000=*
   ```

2. Wenn Sie Ressourcen aus einem eingebundenen Dateisystem eines bestimmten Typs, der weder NFS noch Samba ist (z. B. `parsecfs`), in den Untersuchungsbereich aufnehmen möchten, geben Sie den Dateisystemtyp im Parameter `Path` an: Path=<file system type>

   Das Programm untersucht alle Ressourcen des angegebenen Gerätedateisystems.

   Beispiel

   ```
   kesl-control --set-settings 2 ScanScope.item_0002.UseScanArea=Yes ScanScope.item_0002.Path=parsecfs
   ```

   Die folgenden Einstellungen für den Untersuchungsbereich werden der Aufgabe hinzugefügt:

   ```
   [ScanScope.item_0002]
   AreaDesc=All objects
   UseScanArea=Yes
   Path=parsecfs
   AreaMask.item_0000=*
   ```

3. Um die aktuellen Werte der Aufgabeneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --get-settings 2
   ```

So konfigurieren Sie einen Untersuchungszeitplan

Die Ausführung der Aufgabe *Schadsoftware-Untersuchung* kann die Ressourcenauslastung des Computers erhöhen. Um die Auswirkungen von Kaspersky Endpoint Security auf die Leistung der Computer der Benutzer während der aktiven Nutzung zu minimieren, können Sie die Ausführung der Aufgabe für den günstigsten Zeitpunkt planen.

Wenn die Mitarbeiter in Ihrem Unternehmen beispielsweise feste Arbeitszeiten haben, können Sie die Untersuchung so konfigurieren, dass sie nachts oder am Wochenende ausgeführt wird. Ist die Ausführung der Untersuchung aus irgendeinem Grund nicht möglich (beispielsweise wenn der Computer zu diesem Zeitpunkt ausgeschaltet ist), können Sie festlegen, dass die übersprungene Aufgabe automatisch ausgeführt wird, sobald dies möglich ist.

Wenn Sie den optimalen Zeitplan für die Untersuchung eines Computers nicht bestimmen können, können Sie die Aufgabe *Schadsoftware-Untersuchung* nicht nur zu bestimmten Zeiten, sondern auch abhängig von bestimmten Bedingungen ausführen, beispielsweise beim Start eines Programms, beim Herunterladen von Updates in die Datenverwaltung, beim Erkennen eines Virenangriffs oder beim Abschluss einer anderen Aufgabe. Sie können außerdem die Funktion Wake-on-LAN verwenden, um ausgeschaltete Computer kurz vor dem Start der Aufgabe einzuschalten. Sie können die Untersuchung unter Verwendung von Wake-on-LAN nur für die Aufgabe *Schadsoftware-Untersuchung* in Kaspersky Security Center konfigurieren. Sie können Wake-on-LAN nicht aktivieren, um den Computer über die Programmoberfläche zu untersuchen.

So starten Sie die Aufgabe zur Schadsoftware-Untersuchung in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Untersuchungsaufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Zeitplan** aus.

4. Passen Sie den Zeitplan für die Untersuchungsaufgabe an.

5. Passen Sie je nach gewählter Frequenz die erweiterten Einstellungen des Zeitplans für den Aufgabenstart an (siehe Tabelle unten).

6. Speichern Sie die vorgenommenen Änderungen.

Einstellungen für den Untersuchungszeitplan

Einstellung	Description
Aufgabe starten	**Manuell**. Ein Ausführungsmodus, bei dem die Untersuchung manuell zu einem für Sie geeigneten Zeitpunkt gestartet werden kann. Nach Zeitplan. In diesem Startmodus für die Untersuchungsaufgabe führt das Programm die Untersuchungsaufgabe nach dem von Ihnen erstellten Zeitplan aus. Bei Auswahl dieses Startmodus für die Untersuchungsaufgabe können Sie die Untersuchungsaufgabe auch manuell starten.
Übersprungene Aufgaben starten	Ist das Kontrollkästchen aktiviert, startet Kaspersky Endpoint Security die übersprungene Aufgabe, sobald dies möglich ist. Die Aufgabe kann z. B. übersprungen werden, wenn der Computer zur geplanten Startzeit der Aufgabe ausgeschaltet war. Wenn die App die Möglichkeit erhält, versäumte Aufgaben auszuführen, werden die Aufgaben innerhalb eines bestimmten Zeitraums nach dem Zufallsprinzip ausgeführt, um die Auslastung des Computers gleichmäßig zu verteilen. Wenn dieses Kontrollkästchen deaktiviert ist, führt Kaspersky Endpoint Security übersprungene Aufgaben nicht aus. Stattdessen wird die nächste Aufgabe gemäß dem aktuellen Zeitplan ausgeführt.
Automatische zufällige Verzögerung für Aufgabenstarts verwenden	Wenn dieses Kontrollkästchen aktiviert ist, wird die Aufgabe nicht streng nach Zeitplan ausgeführt, sondern zufällig in einem bestimmten Intervall, d. h. die Aufgabenstarts werden zeitlich verteilt. Zufällige Startzeiten verhindern, dass viele Computer gleichzeitig auf den Administrationsserver zugreifen, wenn die Aufgabe nach Zeitplan ausgeführt wird. Der Bereich der zufälligen Startzeiten wird beim Erstellen der Aufgabe automatisch berechnet. Dabei wird die Anzahl der Computer berücksichtigt, denen die Aufgabe zugewiesen ist. Anschließend wird die Aufgabe immer zur berechneten Startzeit ausgeführt. Die berechnete Startzeit ändert sich aber, wenn die Aufgabeneinstellungen geändert werden oder die Aufgabe manuell ausgeführt wird. Wenn das Kontrollkästchen deaktiviert ist, wird die Aufgabe exakt zum geplanten Zeitpunkt ausgeführt.
Automatische zufällige Verzögerung des Aufgabenstarts innerhalb eines Intervalls von	Wenn dieses Kontrollkästchen aktiviert ist, wird die Aufgabe auf Computern innerhalb eines bestimmten Zeitraums zu einem zufälligen Zeitpunkt ausgeführt. Zufällige Startzeiten verhindern, dass viele Computer gleichzeitig auf den Administrationsserver zugreifen, wenn die Aufgabe nach Zeitplan ausgeführt wird. Wenn das Kontrollkästchen deaktiviert ist, wird die Aufgabe exakt zum geplanten Zeitpunkt ausgeführt.
Vor dem Aufgabenstart die Geräte mittels Wake-On-LAN hochfahren	Wenn dieses Kontrollkästchen aktiviert ist, erhält das Betriebssystem des Computers eine bestimmte Vorlaufzeit für seinen Start, bevor die Aufgabe ausgeführt wird. Standardmäßig beträgt die Vorlaufzeit 5 Minuten. Aktivieren Sie das Kontrollkästchen, wenn Sie die Aufgabe auf allen Computern ausführen möchten, auch auf ausgeschalteten Computern.

Einstellung	Description
Geräte nach Abschluss der Aufgabe herunterfahren	Wenn dieses Kontrollkästchen aktiviert ist, wird der Computer nach Abschluss der Aufgabe heruntergefahren. Sie können diese Funktion beispielsweise aktivieren, um den Computer freitags nach Feierabend untersuchen zu lassen. Nach Abschluss der Aufgabe schaltet das Programm den Computer für das Wochenende aus.
Aufgabe unterbrechen, wenn deren Ausführung länger dauert als	Ausführungszeit der Aufgabe begrenzen. Nach Ablauf des festgelegten Zeitraums bricht Kaspersky Endpoint Security die Aufgabe ab. Die Aufgabe wird nicht als abgeschlossen markiert. Wenn Kaspersky Endpoint Security die Aufgabe das nächste Mal ausführt, wird sie von vorne gestartet und wie geplant ausgeführt.

So planen Sie die Aufgabe zur Schadsoftware-Untersuchung über die Befehlszeile

Um die Aufgabe einmalig zu einem bestimmten Zeitpunkt auszuführen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-schedule 2 RuleType=Once StartTime='<year>/<month>/<day of the month> <hh>:<mm>:<ss>'
```

Um die Aufgabe monatlich auszuführen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-schedule 2 RuleType=Monthly StartTime='<hh>:<mm>:<ss>;<day of the month>'
```

Um die Aufgabe an einem bestimmten Wochentag auszuführen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-schedule 2 RuleType=Weekly StartTime='<hh>:<mm>:<ss>;<day of the week>'
```

Um die Aufgabe in regelmäßigen Abständen (in Tagen) auszuführen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-schedule 2 RuleType=Daily StartTime='<hh>:<mm>:<ss>;<interval between runs (in days)>'
```

Um die Aufgabe ab einem bestimmten Datum in regelmäßigen Abständen (in Stunden) auszuführen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-schedule 2 RuleType=Hourly StartTime='<year>/<month>/<day of the month> <hh>:<mm>:<ss>;
<interval between runs (in hours)>'
```

Um die Aufgabe ab einem bestimmten Datum in regelmäßigen Abständen auszuführen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-schedule 2 RuleType=Minutely StartTime='<hh>:<mm>:<ss>;<interval between runs (in minutes)>'
```

Um die Aufgabe sofort nach dem Programmstart auszuführen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-schedule 2 RuleType=PS
```

Um die Aufgabe sofort nach dem Update der Datenbanken auszuführen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-schedule 2 RuleType=BR
```

Um die Zeitplanung für die Aufgabe zu deaktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-schedule 2 RuleType=Manual
```

Um zusätzliche Einstellungen des Aufgabenzeitplans zu verwalten, führen Sie den folgenden Befehl aus:

```
kesl-control --set-schedule 2 RandomInterval=<time interval (minutes)> RunMissedStartRules=<Yes|No>
UseWorkingTimeout=<Yes|No> WorkingTimeout=<maximum task completion time (minutes)> QueueScanTasks=<Yes|No>
```

```
Um die aktuellen Werte der Aufgabeneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

kesl-control --get-schedule 2
```

Symbole

Einstellungen des Zeitplans für den Aufgabenstart

Einstellung	Description
`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 Anwendung starten. • `BR` – Aufgabe nach dem Update der Anwendungsdatenbanken starten.
`StartTime`	Datum und Uhrzeit des Aufgabenstarts. Das Format dieser Einstellung hängt von `RuleType` ab. Mögliche Werte: • `<year>`: 1970 bis 2099 • `<month>`: JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC. • `<day of the month>`: 1 bis 31 • `<day of the week>`: Mon, Tue, Wed, Thu, Fri, Sat, Sun. • `<hh>`: 0 bis 23 • `<mm>`: 0 bis 59 • `<ss>`: 0 bis 59 • `<interval between runs (in days)>`: 0 bis 364 • `<interval between runs (in hours)>`: 0 bis 23 • `<interval between runs (in minutes)>`: 0 bis 59
`RandomInterval`	Führen Sie die Aufgabe auf den Computern zu einem zufälligen Zeitpunkt innerhalb eines bestimmten Zeitintervalls (von 0 bis zum angegebenen Wert) aus. Dadurch wird vermieden, dass mehrere Aufgaben gleichzeitig gestartet werden. Standardwert: 99 Minuten. Zulässige Werte: 0 – 999.
`RunMissedStartRules`	Start einer übersprungenen Aufgabe nach dem Starten der App. • `Yes` (Standardwert) bedeutet, dass die Ausführung einer verpassten Aufgabe aktiviert ist. Wenn das Programm angehalten oder der Computer ausgeschaltet wird, während eine geplante Aufgabe ausgeführt wird, startet Kaspersky Endpoint Security diese Aufgabe sofort nach dem Start des Programms. So können Sie sicherstellen, dass kritische Aufgaben niemals verpasst werden. • `No` bedeutet, dass die Ausführung einer verpassten Aufgabe deaktiviert ist. Wenn das Programm angehalten oder der Computer ausgeschaltet wird, während eine geplante Aufgabe ausgeführt wird, überspringt das Programm diese Aufgabe. Dadurch wird eine zusätzliche Belastung beim Start des Programms vermieden.
`UseWorkingTimeout`	Stoppen der Aufgabe, wenn die durch den Parameter `WorkingTimeout` angegebene maximale Ausführungszeit der Aufgabe erreicht ist. Die Aufgabe wird auch dann gestoppt, wenn sie noch nicht abgeschlossen ist. Der nächste Aufgabenstart wird entsprechend des Zeitplans durchgeführt. • `Yes` – Stoppt die Aufgabe, wenn deren maximale Ausführungszeit erreicht wurde. • `No` (Standardwert) – Stoppt die Aufgabe nicht, wenn deren maximale Ausführungszeit erreicht wurde.

Einstellung	Description
`WorkingTimeout`	Die maximale Ausführungszeit der Aufgabe (in Minuten). Beim Erreichen dieses Wertes wird die Ausführung der Aufgabe von der Anwendung gestoppt, wenn der Wert des Parameters `UseWorkingTimeout=Yes` festgelegt ist. Standardwert: 120 Minuten. Zulässige Werte: 1 – 999.

Beispiel für die Ausführung der Untersuchungsaufgabe alle 10 Stunden

```
kesl-control --set-schedule 2 RuleType=Hourly StartTime='2030/May/28 12:00:00;10'
```

Beispiel für die Ausführung der Untersuchungsaufgabe am 15. jedes Monats

```
kesl-control --set-schedule 2 RuleType=Monthly StartTime='12:00:00;15'
```

Beispiel für die Ausführung der Aufgabe jeden Dienstag

```
kesl-control --set-schedule 2 RuleType=Weekly StartTime='12:00:00;Tue'
```

So untersuchen Sie eine einzelne Datei oder ein Verzeichnis

Kaspersky Endpoint Security bietet die Möglichkeit, mithilfe der Befehlszeile einzelne Dateien auf Viren und andere Malware zu untersuchen. Sie können beispielsweise Archive gezielt untersuchen, für die die Untersuchung im Schutz vor bedrohlichen Dateien standardmäßig deaktiviert ist.

Standardmäßig untersucht das Programm die Datei mithilfe der Aufgabeneinstellungen der Aufgabe *Scan_File (ID: 3)*, die von Kaspersky-Experten empfohlen werden. Die Standardeinstellungen bieten das empfohlene Schutzniveau und eine optimale Ressourcennutzung. Standardmäßig speichert das Programm eine Kopie eines infizierten Objekts im Backup und versucht, das Objekt zu desinfizieren. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), löscht die Anwendung das Objekt. Sie können beim Erkennen einer Bedrohung eine andere Aktion auswählen und andere Aufgabeneinstellungen verwalten.

So starten Sie die Untersuchung einer einzelnen Datei oder eines Verzeichnisses über die Befehlszeile

```
kesl-control --scan-file <path to the file or directory>
```

Daraufhin erstellt Kaspersky Endpoint Security einen Bericht in der folgenden Form:

```
Untersuchte Objekte: N

Gefundene Objekte gesamt: N

Infizierte und andere Objekte: N

Desinfizierte Objekte: N

In den Backup-Speicher verschoben: N

Entfernte Objekte: N

Nicht desinfizierte Objekte: N

Untersuchungsfehler: N
```

```
Kennwortgeschützte Objekte: N

Übersprungene Objekte: N

Von Cloud Sandbox entdeckt: N
```

So optimieren Sie Aufgaben zur benutzerdefinierten Untersuchung

Zur Optimierung von benutzerdefinierten Untersuchungen können Sie den gleichzeitigen Start mehrerer Aufgaben einschränken. Wenn ein Benutzer versucht, zu viele Aufgaben zur benutzerdefinierten Untersuchung gleichzeitig auszuführen, führt das Programm die Aufgaben, die das Limit überschreiten, nicht aus. So können Sie die Nutzung der Ressourcen des Client-Geräts steuern und beispielsweise eine übermäßige Auslastung des Servers vermeiden. Standardmäßig ist das Limit für die Anzahl der Aufgaben zur benutzerdefinierten Untersuchung auf 100 festgelegt.

Kaspersky Endpoint Security beschränkt Aufgaben nur für unprivilegierte Benutzer. Ein Benutzer mit Root-Berechtigungen kann Aufgaben zur benutzerdefinierten Untersuchung ohne Einschränkungen ausführen.

Sie können das Limit für Aufgaben zur benutzerdefinierten Untersuchung über die Befehlszeile mithilfe von allgemeinen Programmeinstellungen konfigurieren. Sie können das Aufgabenlimit nicht in der Verwaltungskonsole oder in der Web Console konfigurieren.

So optimieren Sie Aufgaben zur benutzerdefinierten Untersuchung über die Befehlszeile

```
kesl-control --set-app-settings LimitNumberOfScanFileTasks=<number of tasks>
```

Untersuchung wichtiger Bereiche.

Mit einer speziellen Untersuchungsaufgabe können Sie nur wichtige Bereiche des Computers untersuchen: *Untersuchung kritischer Bereiche*. Die *Untersuchung kritischer Bereiche* untersucht schnell die Bereiche des Computers, in denen Malware am häufigsten gefunden wird. Der Untersuchungsbereich dieser Aufgabe umfasst Bootsektoren, Autostart-Objekte, Kernel-Speicher und laufende Prozesse.

Malware, der es gelingt, wichtige Bereiche des Computers zu kompromittieren, kann ihre Funktionen ausführen und dabei der Erkennung entgehen. Standardmäßig führt das Programm die Aufgabe mit den von Kaspersky-Experten empfohlenen Einstellungen aus. Die Standardeinstellungen bieten das empfohlene Schutzniveau und eine optimale Ressourcennutzung.

Kaspersky-Experten empfehlen, die Standardeinstellungen der Aufgabe *Untersuchung kritischer Bereiche* nicht zu ändern.

Wenn der Root-Benutzer keinen Zugriff auf ein Remote-Verzeichnis hat, das auf dem Gerät über das NFSv4-Protokoll eingebunden ist, überspringt das Programm diese Datei während der Untersuchung.

Der Assistent für die Ersteinrichtung des Administrationsservers erstellt automatisch eine Aufgabe *Untersuchung kritischer Bereiche*. Um eine Aufgabe *Untersuchung kritischer Bereiche* zu erstellen, installieren Sie während der Ausführung des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Linux. Bei Bedarf können Sie Benutzeraufgaben vom Typ *Untersuchung kritischer Bereiche* erstellen.

So starten Sie eine Untersuchung wichtiger Bereiche in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** den Eintrag **Kaspersky Endpoint Security für Linux** aus.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Untersuchung kritischer Bereiche**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, zum Beispiel *Untersuchung wichtiger Bereiche nach einer Computerinfektion*.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Wechseln Sie zum nächsten Schritt.

5. Schließen Sie den Assistenten ab.

6. Klicken Sie auf die Untersuchungsaufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

7. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

8. Passen Sie die Untersuchungsaufgabe an (siehe Tabelle unten).

9. Konfigurieren Sie bei Bedarf auf der Registerkarte **Zeitplan** die Einstellungen für den Zeitplan für den Aufgabenstart.

10. Speichern Sie die vorgenommenen Änderungen.

11. Starten Sie die Untersuchungsaufgabe.

Einstellungen der Aufgabe Untersuchung wichtiger Bereiche

Einstellung	Description
Untersuchungsbereich	Eine Tabelle mit Bereichen, die von der Aufgabe untersucht werden sollen. Standardmäßig umfasst der Untersuchungsbereich alle Verzeichnisse des lokalen Dateisystems, den Kernel-Speicher, den Speicher laufender Prozesse, Autostart-Objekte und Bootsektoren.
Aktion beim Fund einer Bedrohung	• **Desinfizieren – Löschen, wenn Desinfektion fehlschlägt** (Standardeinstellung). Wenn Sie diese Aktion auswählen, versucht die Anwendung, das infizierte Objekt zu desinfizieren, indem sie eine Kopie des Objekts im Backup-Speicher speichert. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), löscht die Anwendung das Objekt. • **Desinfizieren – Informieren, wenn Desinfektion fehlschlägt**. Wenn Sie diese Aktion auswählen, versucht die Anwendung, das infizierte Objekt zu desinfizieren, indem sie eine Kopie des Objekts im Backup-Speicher speichert. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), speichert die Anwendung Informationen darüber im Protokoll. • **Informieren**. Wenn Sie diese Aktion auswählen, speichert die Anwendung Informationen über das infizierte Objekt im Protokoll.

Einstellung	Description
Archive untersuchen	Wenn diese Option aktiviert ist, untersucht das Programm Archive. Die Anwendung 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. Um ein Archiv zu untersuchen, muss es zunächst von der Anwendung entpackt werden, was die Untersuchung verlangsamen kann. Sie können die Dauer der Untersuchung von Archiven verkürzen, indem Sie die Einstellungen **Datei überspringen, wenn Untersuchung länger dauert als (Sek.)** und **Dateien nicht untersuchen, wenn größer als (MB)** festlegen. Diese Option ist standardmäßig deaktiviert.
Programmpakete und selbstextrahierende Archive untersuchen	Wenn diese Option aktiviert ist, untersucht das Programm selbstentpackende Archive. Selbstentpackende Archive sind Archive, die ein ausführbares Modul zum Entpacken enthalten. Diese Option ist standardmäßig deaktiviert.
Dateien in E-Mail-Formaten untersuchen	E-Mail-Nachrichten im Nur-Text-Format untersuchen. Die Funktion ist standardmäßig deaktiviert.
E-Mail-Datenbanken untersuchen	Wenn diese Option aktiviert ist, untersucht das Programm Mail-Datenbanken von Microsoft Outlook, Outlook Express, The Bat! und anderen Mail-Anwendungen. Die Funktion ist standardmäßig deaktiviert.
Dateien nicht untersuchen, wenn größer als (MB)	Sie können die maximale Größe einer Datei, die untersucht werden kann, in Megabyte angeben. Zulässige Werte: 0 – 9999. Ist der Wert 0 angegeben, untersucht die Anwendung Dateien jeder Größe. Die Funktion ist standardmäßig deaktiviert.
Datei überspringen, wenn Untersuchung länger dauert als (Sek.)	Sie können die maximale Untersuchungsdauer für eine Datei in Sekunden angeben. Nach Ablauf des angegebenen Zeitraums bricht die Anwendung die Untersuchung der Datei ab. Zulässige Werte: 0 – 9999. Ist der Wert 0 angegeben, dann ist die Untersuchungsdauer nicht beschränkt. Die Funktion ist standardmäßig deaktiviert.
Nicht mehrere Untersuchungsaufgaben gleichzeitig ausführen	Aufgeschobener Start von Untersuchungsaufgaben, wenn bereits eine Untersuchungsaufgabe ausgeführt wird. Kaspersky Endpoint Security reiht neue Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Beispiel: Das Programm hat nach Zeitplan eine vollständige Untersuchungsaufgabe gestartet. Wenn ein Benutzer versucht, eine schnelle Untersuchung über die Programmoberfläche zu starten, stellt Kaspersky Endpoint Security diese Aufgabe zur schnellen Untersuchung in die Warteschlange und startet diese Aufgabe automatisch, nachdem die vollständige Untersuchungsaufgabe abgeschlossen wurde. Die Funktion ist standardmäßig deaktiviert.
iChecker-Technologie verwenden	Wenn diese Option aktiviert ist, untersucht das Programm nur neue Dateien sowie Dateien, die nach der letzten Untersuchung geändert wurden. Wenn diese Option deaktiviert ist, untersucht das Programm Dateien unabhängig von ihrem Erstellungs- oder Änderungsdatum. Diese Option ist standardmäßig deaktiviert.

So führen Sie die Aufgabe „Untersuchung wichtiger Bereiche“ über die Befehlszeile aus

1. Konfigurieren Sie bei Bedarf die Aufgabeneinstellungen (s. folgende Tabelle).

   ```
   kesl-control --set-settings 4 <setting name>=<setting value>
   ```

2. Konfigurieren Sie bei Bedarf den Zeitplan für die Aufgabe.

3. Um die aktuellen Werte der Aufgabeneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --get-settings 4 [--json]
   ```

   Wobei gilt: `--json` – Gibt Daten im JSON-Format aus.

4. Um die Aufgabe auszuführen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --start-task 4 [-W] [--progress]
   ```

Wobei gilt:

- `[-W]` aktiviert die Ausgabe aktueller Ereignisse, die sich auf die Aufgabe beziehen.
- `[--progress]` – Fortschritt der laufenden Aufgabe anzeigen.

Bei Bedarf können Sie Benutzeraufgaben erstellen vom Typ *Untersuchung wichtiger Bereiche*.

Einstellungen der Aufgabe Untersuchung wichtiger Bereiche

Einstellung	Description	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) – Prozessspeicher und Kernelspeicher untersuchen. `No` – Prozessspeicher und Kernelspeicher nicht untersuchen.
`ScanStartupObjects`	Aktiviert die Untersuchung der Autostart-Objekte.	`Yes` (Standardwert) – Autostart-Objekte untersuchen. `No` – Autostart-Objekte nicht untersuchen.
`ScanArchived`	Aktiviert die Untersuchung von Archiven (einschließlich selbstentpackender sfx-Archive). Die Anwendung 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 untersuchen. Wenn für den Parameter `ActionOnThreat` der Wert `DisinfectDeleteIfNotPossible` angegeben und eine Desinfizierung nicht möglich ist, löscht die Anwendung je nach Archivtyp entweder das infizierte Objekt oder das gesamte Archiv, das die Bedrohung enthält. `No` – Archive nicht untersuchen.
`ScanSfxArchived`	Aktiviert die Untersuchung ausschließlich von self-extracting archives (Archiven, die ein ausführbares Entpackmodul enthalten).	`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 Format plain text.	`Yes` – E-Mail-Nachrichten im Nur-Text-Format untersuchen. `No` (Standardwert) – E-Mail-Nachrichten im 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.

Einstellung	Description	Werte
`QueueScanTasks`	Geplante Untersuchungsaufgaben verzögern, wenn eine zuvor gestartete geplante Untersuchung noch ausgeführt wird. Kaspersky Endpoint Security reiht geplante Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Eine Untersuchungsaufgabe soll beispielsweise um 18:00 Uhr und um 20:00 Uhr ausgeführt werden. Die für 20:00 Uhr geplante Untersuchungsaufgabe wird verzögert, wenn die Untersuchung um 18:00 Uhr noch ausgeführt wird. Die verzögerte Aufgabe wird ausgeführt, nachdem die Aufgabe um 18:00 Uhr beendet wurde.	`Yes`, um geplante Untersuchungsaufgaben in die Warteschlange einzureihen, wenn die aktuelle Untersuchung noch ausgeführt wird. `No` (Standardwert), um geplante Untersuchungsaufgaben auch dann auszuführen, wenn die aktuelle Untersuchung noch ausgeführt wird.
`ActionOnThreat`	Auswahl der Aktion, welche die Anwendung für infizierte Objekte ausführen soll.	`DisinfectDeleteIfNotPossible` (Desinfizieren. Entfernen, wenn Desinfektion fehlschlägt) – Die Anwendung versucht, das infizierte Objekt zu desinfizieren und speichert eine Kopie des Objekts im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), löscht die Anwendung das Objekt. `DisinfectInformIfNotPossible` (Desinfizieren. Informieren, wenn Desinfektion fehlschlägt) – Die Anwendung versucht, das infizierte Objekt zu desinfizieren und speichert eine Kopie des Objekts im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), speichert die Anwendung Informationen darüber im Protokoll. `Inform` (Informieren) – Die Anwendung unternimmt keinen Versuch, das infizierte Objekt zu desinfizieren oder zu löschen. Informationen über das infizierte Objekt werden im Protokoll gespeichert. Der Standardwert ist: `DisinfectDeleteIfNotPossible`.
`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, von Untersuchungen ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht von der Untersuchung ausschließen.

`ExcludeMasks.item_#`	Ausnahme 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 die Werte 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, aus der Untersuchung.	`Yes` – Objekte, welche die in der Einstellung `ExcludeThreats.item_#` angegebenen Bedrohungen enthalten, von der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die Bedrohungen enthalten, die in der Einstellung `ExcludeThreats.item_#` angegeben sind, nicht von der Untersuchung ausschließen.

Einstellung	Description	Werte

`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 verwenden, um Informationen über Ihr Netzwerk zu erhalten. 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 Anwendung 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` – Globale Ausnahmen nicht verwenden.
`UseOASExclusions`	Aktivieren der Verwendung der Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der Untersuchung.	`Yes` (Standardwert) – Ausschlüsse aus dem Schutz vor bedrohlichen Dateien verwenden. `No` – Ausnahmen für den Schutz vor bedrohlichen Dateien nicht 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 untersuchte Objekte in Archiven 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. 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.

Einstellung	Description	Werte
`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 mit minimaler Belastung des Systems. `Medium` – Eine mittlere Stufe der heuristischen Analyse bei ausgewogener Systemauslastung. `Deep` – Die gründlichste Untersuchung bei maximaler Systemauslastung. `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 Gerätenamen. Die App untersucht die Bootsektoren dieser Geräte. Der Einstellungswert darf nicht leer sein. Um die Aufgabe auszuführen, müssen Sie mindestens eine Maske für Gerätenamen angeben.	`AllObjects` – Untersuchung der Bootsektoren aller Geräte. `<device name mask>` – Bootsektoren der Geräte untersuchen, deren Namen der angegebenen Maske entsprechen. Standardwert: `/**` (beliebiger Zeichensatz im Gerätenamen, einschließlich des Zeichens `/`)
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.	Der Standardwert ist: `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 Anwendung 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_<item number>=*doc`

Einstellung	Description	Werte
`Path`	Pfad zum Verzeichnis mit untersuchten Objekten.	`<path to local directory>` – Objekte in dem angegebenen Verzeichnis untersuchen. Standardmäßige Pfadangabe `/` – Die Anwendung untersucht alle Verzeichnisse des lokalen Dateisystems. `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. `<file system type>` – Alle Ressourcen des angegebenen Dateisystemgeräts 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 Anwendung 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 ausschließen)

Einstellung	Description	Werte
`Path`	Pfad zum Verzeichnis mit ausgeschlossenen Objekten.	`<path to local directory>` – Objekte im angegebenen Verzeichnis (einschließlich Unterverzeichnissen) von Untersuchungen ausschließen. Bei der Angabe des Pfades können Masken verwendet werden. 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/`. Der Pfad `/` ist standardmäßig angegeben. Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus. `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. `<file system type>` – Alle Ressourcen des angegebenen Dateisystemgeräts von der Untersuchung ausschließen. Remote-Verzeichnisse werden nur dann von der Untersuchung durch die Anwendung ausgeschlossen, wenn sie bereits vor dem Aufgabenstart eingebunden wurden. Remote-Verzeichnisse, die erst nach dem Aufgabenstart eingebunden wurden, werden von der Untersuchung nicht ausgeschlossen.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Container untersuchen

Kaspersky Endpoint Security kann Container und Images in Echtzeit oder auf Befehl auf Malware untersuchen.

Um die Funktion zur Untersuchung von Containern nutzen zu können, benötigen Sie eine Lizenz, in der diese Funktion enthalten ist.

Die Komponente ist für Geräte mit Elbrus-CPU nicht verfügbar.

Container-Überwachung

Die Komponente *Container-Überwachung* untersucht laufende Container und Namensräume in Echtzeit. Standardmäßig ist die Komponente "Container-Überwachung" aktiviert.

Damit die Komponente "Container-Überwachung" funktioniert, muss die Komponente Schutz vor bedrohlichen Dateien aktiviert sein. Bei der Untersuchung von Containern und Namensräumen werden die Einstellungen des Schutzes vor bedrohlichen Dateien verwendet.

Das empfohlene Konfigurationsszenario für die Container-Überwachung umfasst folgende Schritte:

1. **Integration des Programms mit Tools zur Containerverwaltung konfigurieren**

   Das Programm unterstützt die Integration in das Container-Management-System Docker, in die CRI-O-Umgebung sowie in die Dienstprogramme Podman und runc.

2. **Schutzbereich erstellen**

   Legen Sie die Geräte fest, auf denen Sie Container und Namensräume untersuchen möchten.

3. **Wählen Sie in den Einstellungen für die Container-Überwachung die Aktion „Container überspringen“ aus**

   Wenn in einem Container ein infiziertes Objekt gefunden wird, kann Kaspersky Endpoint Security den Container sofort anhalten, keine Aktion ausführen oder den Container anhalten, wenn die Desinfektion des Objekts oder die Beseitigung der Bedrohung nicht möglich ist. Wählen Sie die Aktion **Container überspringen** aus, um die Komponente zu testen. Das Programm führt beim Erkennen eines infizierten Objekts keine Aktion für den Container aus, protokolliert jedoch Informationen über erkannte Bedrohungen.

4. **Statistiken zur Container-Überwachung erfassen**

   Sie können Statistiken zur Container-Überwachung mithilfe von Berichten abrufen.

5. **Wählen Sie die Aktion aus, die beim Erkennen eines infizierten Objekts für einen Container ausgeführt werden soll.**

   Sie können eine Aktion auswählen, die von der Anwendung beim Fund eines infizierten Objekts für den Container ausgeführt werden soll.

Untersuchung von Containern auf Befehl

Das Programm kann Container und Images bei Bedarf auf Viren und andere Malware untersuchen. Dies erfolgt mithilfe der vordefinierten Aufgabe *Untersuchung von Containern (Container_Scan)*. Sie können die vordefinierte Aufgabe konfigurieren oder Benutzeraufgaben zum Untersuchen von Containern über die Befehlszeile, in der Web Console oder in der Verwaltungskonsole erstellen.

Die Anwendung kann mehrere Aufgaben zur Untersuchung von Containern gleichzeitig ausführen.

Das empfohlene Konfigurationsszenario für die Untersuchung von Containern umfasst folgende Schritte:

1. **Integration des Programms mit Tools zur Containerverwaltung konfigurieren**

   Das Programm unterstützt die Integration in das Container-Management-System Docker, in die CRI-O-Umgebung sowie in die Dienstprogramme Podman und runc.

2. **Untersuchungsbereich einrichten**

   Standardmäßig untersucht das Programm alle Container auf einem geschützten Gerät. Wenn Sie nur einzelne Container untersuchen möchten, können Sie deren Namen oder Namensmasken angeben.

3. **Wählen Sie in den Einstellungen für die Untersuchung von Containern die Aktionen „Container überspringen“ und „Image überspringen“ aus**

   Wenn in einem Container ein infiziertes Objekt gefunden wird, kann Kaspersky Endpoint Security den Container sofort anhalten, keine Aktion ausführen oder den Container anhalten, wenn die Desinfektion des Objekts oder die Beseitigung der Bedrohung nicht möglich ist. Wenn im Container-Image ein infiziertes Objekt erkannt wird, kann Kaspersky Endpoint Security das Container-Image löschen oder keine Aktion für das Container-Image ausführen. Wählen Sie die Aktionen **Container überspringen** und **Image überspringen** aus, um die Aufgabe zu testen. Wenn ein infiziertes Objekt erkannt wird, führt das Programm keine Aktion für den Container und das Image aus, protokolliert jedoch Informationen über erkannte Bedrohungen.

4. **Statistiken zur Untersuchung von Containern erfassen**

   Sie können Statistiken zur Untersuchung von Containern mithilfe von Berichten abrufen.

5. **Programmleistung optimieren**

   Optimieren Sie nach der Analyse der gesammelten Informationen die Leistung des Programms:

   - Globale Ausnahmen hinzufügen
   - Untersuchungsausnahmen hinzufügen
   - Untersuchung von Containern optimieren

6. **Aktion auswählen, die beim Erkennen eines infizierten Objekts für einen Container und dessen Image ausgeführt werden soll**

   Wählen Sie die Aktionen aus, die das Programm für einen Container und dessen Image ausführt, wenn es ein infiziertes Objekt erkennt.

Benutzerdefinierte Untersuchung von Containern

Die Aufgabe vom Typ *Benutzerdefinierte Untersuchung von Containern* ermöglicht das Konfigurieren und Speichern von Einstellungen, die beim Untersuchen der angegebenen Container und Images mithilfe des folgenden Befehls verwendet werden:

```
kesl-control --scan-container
```

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).

Der Befehl erstellt eine temporäre Aufgabe zum Untersuchen von Containern und Images und führt sie aus. Diese Aufgabe wird nach Abschluss automatisch gelöscht. Gleichzeitig werden die Ergebnisse der Untersuchung in die Konsole ausgegeben.

Besonderheiten und Einschränkungen

- Die Anwendung prüft keine Namensräume und Container, es sei denn, auf dem Betriebssystem sind Komponenten für die Arbeit mit Containern und Namensräumen installiert. In diesem Fall wird der Status der Komponente "Container-Überwachung" über die Befehlszeile als "Aufgabe ist verfügbar und wird nicht ausgeführt" angezeigt, während er in Kaspersky Security Center als "Beendet" angezeigt wird.
- Eine Aktion der Container-Überwachung kann nur ausgewählt werden, wenn die Lizenz des Programms diese Funktion umfasst.

So konfigurieren Sie die Integration mit Tools zur Containerverwaltung

Das Programm unterstützt die Integration in das Container-Management-System Docker, in die CRI-O-Umgebung sowie in die Dienstprogramme Podman und runc. Sie können die Integration mit diesen Tools zur Containerverwaltung konfigurieren.

So konfigurieren Sie die Integration mit Tools zur Containerverwaltung in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Einstellungen der Untersuchung von Containern**.
5. Stellen Sie sicher, dass sich der Umschalter für die Komponente "Container-Überwachung" in der Position **Überwachung von Namespaces und Containern AKTIVIERT** befindet.

6. Klicken Sie im Block **Einstellungen der Untersuchung von Containern** auf **Konfigurieren**.

7. Daraufhin wird das Fenster **Untersuchungseinstellungen** geöffnet. Aktivieren Sie in diesem Fenster die Kontrollkästchen neben den Tools zur Containerverwaltung, die im Betriebssystem der geschützten Geräte installiert sind und verwendet werden, und verwalten Sie anschließend bei Bedarf die Einstellungen:

   - Das Kontrollkästchen **Docker verwenden** aktiviert das Docker-System zur Containerverwaltung. Dieses Kontrollkästchen ist standardmäßig aktiviert.

     - **Pfad zum Docker-Socket** ist ein Eingabefeld für den Pfad oder URI (Uniform Resource Identifier) des Docker-Sockets. Der Standardwert ist /var/run/docker.sock.

   - Das Kontrollkästchen **CRI-O verwenden** aktiviert die CRI-O-Umgebung. Dieses Kontrollkästchen ist standardmäßig aktiviert.

     - **Dateipfad** ist ein Eingabefeld für den Pfad zur CRI-O-Konfigurationsdatei. Standardwert: /etc/crio/crio.conf.

   - Das Kontrollkästchen **Podman verwenden** aktiviert das Podman-Tool. Dieses Kontrollkästchen ist standardmäßig aktiviert.

     - **Dateipfad** ist ein Eingabefeld für den Pfad zur ausführbaren Datei des Podman-Tools. Der Standardwert ist /usr/bin/podman.

     - **Stammverzeichnis** ist ein Eingabefeld für den Pfad zum Stammverzeichnis des Container-Speichers.

   - Das Kontrollkästchen **runc verwenden** aktiviert das runc-Tool. Dieses Kontrollkästchen ist standardmäßig aktiviert.

     - **Dateipfad** ist ein Eingabefeld für den Pfad zur ausführbaren Datei des runc-Tools. Der Standardwert ist /usr/bin/runc.

     - **Stammverzeichnis** ist ein Eingabefeld für den Pfad zum Stammverzeichnis des Speichers für den Container-Status. Der Standardwert ist /run/runc.

8. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Integration mit Tools zur Containerverwaltung über die Befehlszeile

Über die Befehlszeile können Sie die Echtzeitüberwachung von Namespaces und Containern mithilfe der Einstellung `NamespaceMonitoring=<Yes|No>` aus den allgemeinen App-Einstellungen aktivieren oder deaktivieren.

Sie können den Wert der Einstellung `NamespaceMonitoring` mithilfe der Konfigurationsdatei, die alle allgemeinen Anwendungseinstellungen enthält, oder mithilfe von Befehlszeilenschaltern ändern.

Überwachung von Namespaces und Containern mithilfe von Befehlszeilenoptionen aktivieren

```
kesl-control --set-app-settings NamespaceMonitoring=Yes
```

Bei der Echtzeituntersuchung von Namespaces und Containern werden die Einstellungen für die Untersuchung von Containern angewendet. Sie können diese Einstellungen mithilfe spezieller Verwaltungsbefehle für Kaspersky Endpoint Security anzeigen und ändern:

- Sie können die aktuellen Werte der Einstellungen für die Untersuchung von Containern in die Konsole oder in eine Konfigurationsdatei ausgeben. Mit dieser Datei können Sie Einstellungen ändern.
- Sie können alle Einstellungen für die Untersuchung von Containern mithilfe der Konfigurationsdatei ändern, welche die Einstellungen enthält. Sie können die Konfigurationsdatei mit dem Befehl zur Ausgabe der allgemeinen Einstellungen für die Untersuchung von Containern abrufen.
- Sie können einzelne Einstellungen mithilfe von Befehlszeilenoptionen im Format `<setting name>=<setting value>` verwalten. Mit einem Befehl zur Ausgabe der Einstellungen für die Untersuchung von Containern können Sie die aktuellen Werte der Einstellungen abrufen.

```
Aktuelle Werte der Einstellungen für die Untersuchung von Containern in die Konsole ausgeben

kesl-control --get-container-settings [--json]
```

Dabei wird `--json` angegeben, um die Einstellungen im JSON-Format auszugeben. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

```
Aktuelle Werte der Einstellungen für die Untersuchung von Containern in eine Datei ausgeben

kesl-control --get-container-settings --file <path to configuration file> [--json]
```

Wobei gilt:

- `--file <path to configuration file>` ist der Pfad zu der Datei, in der Sie die Einstellungen für die Untersuchung von Containern speichern 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.
- `--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 für die Untersuchung von Containern mithilfe einer Konfigurationsdatei:

1. Geben Sie die Einstellungen für die Untersuchung von Containern 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 folgenden Befehl aus:

   ```
   kesl-control --set-container-settings --file <path to configuration file> [--json]
   ```

   Wobei gilt:

   - `--file <path to configuration file>` ist der vollständige Pfad zur Konfigurationsdatei mit den Einstellungen für die Untersuchung von Containern.
   - `--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 Anwendung, 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 für die Untersuchung von Containern werden in die App importiert.

```
Werte der Einstellungen für die Untersuchung von Containern mithilfe von Befehlszeilenoptionen ändern

kesl-control --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Dabei ist `<setting name>=<setting value>` der Name und der Wert einer Einstellung für die Untersuchung von Containern.

Die Werte der angegebenen Einstellungen für die Untersuchung von Containern werden geändert.

So erstellen Sie einen Untersuchungsbereich für die Untersuchung von Containern und Images auf Befehl

Untersuchungsbereich

Ein *Untersuchungsbereich* ist eine Liste mit Namen von Containern, die Kaspersky Endpoint Security während der Ausführung der Aufgabe *Untersuchung von Containern* untersucht.

Standardmäßig untersucht die Aufgabe *Untersuchung von Containern* alle Container auf einem geschützten Gerät. Wenn Sie nur einzelne Container untersuchen möchten, können Sie deren Namen oder Namensmasken angeben.

So erstellen Sie einen Untersuchungsbereich in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Wählen Sie in der Aufgabenliste die Aufgabe „Untersuchung von Containern in Kaspersky Endpoint Security“ aus und klicken Sie auf den Namen der Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Geben Sie unter **Erweiterte Untersuchungseinstellungen → Einstellungen der Untersuchung von Containern** im Feld **Namensmaske** den Namen oder die Namensmaske des Containers ein, den Sie untersuchen möchten. Standardmäßig werden alle Container untersucht.

5. Geben Sie unter **Erweiterte Untersuchungseinstellungen → Image-Untersuchungseinstellungen** im Feld **Namensmaske** den Namen oder die Namensmaske des Container-Images ein, das Sie untersuchen möchten. Standardmäßig werden alle Images untersucht.

6. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie einen Untersuchungsbereich über die Befehlszeile

1. Konfigurieren Sie einen Untersuchungsbereich mithilfe des folgenden Befehls:

   ```
   kesl-control --set-settings <task ID|name> ScanContainers=Yes ContainerNameMask=<container name or mask>
   ScanImages=Yes ImageNameMask=<image name or mask>
   ```

Wobei gilt:

- `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `<container name or mask>` ist der Name oder die Namensmaske des Containers, den Sie untersuchen möchten. Masken werden im Format der Befehlsschnittstelle angegeben. Sie können die Symbole `?` und `*` verwenden. Standardmäßig werden alle Container untersucht.
- `<image name or mask>` ist der Name oder die Namensmaske des Images, das Sie untersuchen möchten. Masken werden im Format der Befehlsschnittstelle angegeben. Sie können die Symbole `?` und `*` verwenden. Standardmäßig werden alle Images untersucht.

2. Sie können einen Untersuchungsbereich auch mithilfe einer Konfigurationsdatei konfigurieren:

   a. Geben Sie die Aufgabeneinstellungen in eine Konfigurationsdatei aus, indem Sie den folgenden Befehl ausführen:

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. Öffnen Sie die Konfigurationsdatei zum Bearbeiten.

   c. Fügen Sie der Datei die folgenden Einstellungen hinzu:

   - `ScanContainers=Yes` aktiviert die Untersuchung der angegebenen Container.
   - `ContainerNameMask=<container name or mask>` ist der Name oder die Namensmaske des Containers, den Sie untersuchen möchten. Masken werden im Format der Befehlsschnittstelle angegeben. Sie können die Symbole `?` und `*` verwenden. Standardmäßig werden alle Container untersucht.

- `ScanImages=Yes` aktiviert die Untersuchung der angegebenen Images.
- `ImageNameMask=<image name or mask>` ist der Name oder die Namensmaske des Images, das Sie untersuchen möchten. Masken werden im Format der Befehlsschnittstelle angegeben. Sie können die Symbole `?` und `*` verwenden. Standardmäßig werden alle Images untersucht.

```
Beispiel für die Untersuchung eines Containers namens my_container

ContainerNameMask=my_container
```

```
Beispiel für die Untersuchung aller Container, deren Namen mit my_container beginnen

ContainerNameMask=my_container*
```

```
Beispiel für die Untersuchung aller Container, deren Namen mit my_ beginnen, dann fünf beliebige Zeichen enthalten, anschließend _container enthalten und mit einer beliebigen Zeichenfolge enden

ContainerNameMask=my_?????_container*
```

```
Beispiel für die Untersuchung von Images mit dem Namen "my_image" und dem Tag "latest"

ImageNameMask=my_image:latest
```

```
Beispiel für die Untersuchung aller Images, deren Namen mit my_image_ beginnen und die einen beliebigen Tag haben

ImageNameMask=my_image*
```

d. Speichern Sie die Änderungen in der Konfigurationsdatei.

e. Importieren Sie die Einstellungen aus der Konfigurationsdatei mithilfe des folgenden Befehls in die Aufgabe:

```
kesl- <task ID|name> --file <path> [--json]
```

Wobei gilt:

- `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--file <path>` ist der vollständige Pfad zur Konfigurationsdatei, aus der Sie die Aufgabeneinstellungen importieren möchten.
- `--json` – Geben Sie diesen Schalter an, wenn Sie Einstellungen aus einer Konfigurationsdatei im JSON-Format importieren. Wenn die Option --json nicht angegeben ist, versucht die App, aus einer INI-Datei zu importieren. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Alle Werte der in der Datei definierten Aufgabeneinstellungen werden in die App importiert.

Untersuchungsausnahmen

Eine *Untersuchungsausnahme* ist eine Kombination von Bedingungen. Sind diese Bedingungen erfüllt, so untersucht Kaspersky Endpoint Security ein Objekt nicht auf Viren und andere bedrohliche Programme. Mithilfe von Untersuchungsausnahmen können Sie mit legitimen Anwendungen arbeiten, die von Angreifern für Kompromittierungen des Computers oder der Benutzerdaten ausgenutzt werden können. Diese Anwendungen selbst verfolgen nicht unbedingt einen schädlichen Zweck, können aber von Angreifern ausgenutzt werden. Ausführliche Informationen zu legitimen Anwendungen, die von Angreifern für Kompromittierungen des Computers oder der Benutzerdaten ausgenutzt werden können, finden Sie auf der Website von Kaspersky Encyclopedia.

Sie können auch bestimmte vertrauenswürdige Verzeichnisse vom Untersuchungsbereich ausschließen, um die App-Leistung zu optimieren.

Objekte können wie folgt von der Untersuchung ausgeschlossen werden:

- **Ausnahmen nach Maske**. Geben Sie einen Dateinamen mit einer Maske ein. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

  Verwenden Sie Masken:

  - Das Zeichen `*` (Sternchen), das als Platzhalter für eine beliebige Zeichenkombination steht, mit Ausnahme der Zeichen `\` und `/` (Trennzeichen für die Namen von Dateien und Verzeichnissen in Pfaden zu Dateien und Verzeichnissen). Beispiel: Die Maske `/dir/*/*.txt` umfasst alle Pfade zu Dateien mit der Erweiterung TXT, die sich in Verzeichnissen innerhalb des Verzeichnisses dir befinden, jedoch nicht in Unterverzeichnissen.

  - Zwei aufeinanderfolgende Zeichen `*` stehen im Datei- oder Verzeichnisnamen als Platzhalter für eine beliebige Zeichenkombination (einschließlich einer leeren Zeichenkombination), einschließlich der Zeichen `\` und `/` (Trennzeichen für die Namen von Dateien und Verzeichnissen in Pfaden zu Dateien und Verzeichnissen). Beispiel: Die Maske `/dir/**/*.txt` umfasst alle Pfade zu Dateien mit der Erweiterung TXT, die sich in Verzeichnissen befinden, die innerhalb des Verzeichnisses dir verschachtelt sind, mit Ausnahme des Verzeichnisses dir selbst.

  - Das Zeichen `?` (Fragezeichen), das als Platzhalter für ein beliebiges Einzelzeichen steht, mit Ausnahme der Zeichen `\` und `/` (Trennzeichen für die Namen von Dateien und Verzeichnissen in Pfaden zu Dateien und Verzeichnissen). Beispiel: Die Maske `/dir/???.txt` umfasst die Pfade zu allen Dateien, die sich im Verzeichnis dir befinden, die Erweiterung TXT haben und deren Name aus drei Zeichen besteht.

- **Ausnahmen nach Bedrohungsname** Geben Sie den Namen des Objekttyps gemäß der Klassifikation von Kaspersky Encyclopedia ein (z. B. `Email-Worm`, `Rootkit` oder `RemoteAdmin`). Möglich sind auch Masken mit dem Zeichen `?` (Platzhalter für ein beliebiges Einzelzeichen) und dem Zeichen `*` (Platzhalter für eine beliebige Anzahl von Zeichen). Beispiel: Bei Angabe der Maske `Client*` schließt das Programm die Objekte `Client-IRC`, `Client-P2P` und `Client-SMTP` von Untersuchungen aus.

Kaspersky Endpoint Security ermöglicht außerdem, Dateien bestimmter Formate von der Untersuchung auszuschließen: Archive, E-Mail-Datenbanken, Textdateien, Datenbank-Protokolldateien.

So fügen Sie Untersuchungsausnahmen in der Web Console hinzu

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Wählen Sie in der Aufgabenliste die Aufgabe „Untersuchung von Containern in Kaspersky Endpoint Security“ aus und klicken Sie auf den Namen der Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Ausschlussbereiche**.
5. Fügen Sie bei Bedarf Ausnahmen nach Maske hinzu:
   a. Klicken Sie im Block **Ausnahmen nach Maske** auf **Hinzufügen**.
   b. Daraufhin wird ein Fenster geöffnet; geben Sie in diesem Fenster Vorlagen für die Namen der Dateien an, die Kaspersky Endpoint Security von der Untersuchung ausschließen soll.
   c. Klicken Sie auf die Schaltfläche **Hinzufügen**.
   Die Ausnahmen werden zur Liste hinzugefügt.
6. Fügen Sie bei Bedarf Ausnahmen nach Bedrohungsname hinzu:
   a. Klicken Sie im Block **Ausnahmen nach Bedrohungsname** auf **Hinzufügen**.
   b. Daraufhin wird ein Fenster geöffnet; geben Sie in diesem Fenster Vorlagen für Bedrohungsnamen an. Die Anwendung blockiert die angegebenen Bedrohungen nicht.

   Wenn Sie beispielsweise ein Tool zur Untersuchung Ihres Netzwerks verwenden, fügen Sie der Liste der Bedrohungen, die von der Untersuchung ausgeschlossen werden sollen, den vollständigen Namen der entsprechenden Bedrohung hinzu.
   Den vollständigen Namen der im Objekt gefundenen Bedrohung finden Sie im Protokoll der Anwendung oder auf der Website https://threats.kaspersky.com.
7. Bei Bedarf können Sie Ausnahmen für jede der Listen importieren oder exportieren:
   - Um die Liste der Ausnahmen zu exportieren, klicken Sie auf die Schaltfläche **Exportieren**.
   Kaspersky Endpoint Security speichert die Datei export.json in Ihrem Standardordner für Downloads.
   - So importieren Sie die Ausnahmeliste:
     a. Klicken Sie auf **Import**.
     b. Wählen Sie die JSON-Datei aus, aus der Sie Ausschlussbereiche importieren möchten.
     c. Öffnen Sie die Datei.
     d. Wählen Sie die Importmethode aus: Ausnahmen zur vorhandenen Liste hinzufügen oder die Liste der Ausnahmen ersetzen.
     e. Speichern Sie die vorgenommenen Änderungen.
     Die Regeln aus der JSON-Datei werden in der Liste angezeigt.
8. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie Untersuchungsausnahmen über die Befehlszeile hinzu

1. Fügen Sie mit dem folgenden Befehl einen Ausschlussbereich hinzu:

```
kesl-control --set-settings <Aufgaben-ID|Name> --add-exclusion <Pfad>
```

wobei:

- `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--add-exclusion <path>` fügt den Pfad zum Verzeichnis mit den 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 in dem Verzeichnis, das durch die Einstellung `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 `Path` 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.

2. Sie können einen Ausschlussbereich auch mithilfe einer Konfigurationsdatei hinzufügen:

   a. Geben Sie die Aufgabeneinstellungen in eine Konfigurationsdatei aus, indem Sie den folgenden Befehl ausführen:

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. Öffnen Sie die Konfigurationsdatei zum Bearbeiten.

   c. Fügen Sie der Datei einen Abschnitt `[ExcludedFromScanScope.item_#]` mit den folgenden Einstellungen hinzu:

   - `AreaDesc` – Beschreibung des Ausschlussbereichs, die zusätzliche Informationen zum Ausschlussbereich enthält.
   - `UseScanArea` – Aktiviert den Ausschluss des angegebenen Bereichs.
   - `Path` ist der Pfad zum Verzeichnis mit den auszuschließenden 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=*
     ```

   d. Sie können mehrere Abschnitte `[ExcludedFromScanScope.item_#]` angeben.

   Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge.

   e. Speichern Sie die Änderungen in der Konfigurationsdatei.

f. Importieren Sie die Einstellungen aus der Konfigurationsdatei mithilfe des folgenden Befehls in die Aufgabe:

```
kesl-control --set-settings <task ID|name> --file <path>
```

3. Bei Bedarf können Sie einen Ausnahmebereich löschen, indem Sie den folgenden Befehl ausführen:

```
kesl-control --set-settings <task ID|name> --del-exclusion <path>
```

wobei:

- `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--del-exclusion <path>` entfernt einen Pfad zu einem Verzeichnis mit Objekten, die von der Untersuchung ausgeschlossen werden sollen.

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.

So optimieren Sie die Untersuchung von Containern

Konfigurieren Sie die Untersuchung von Dateien, um die Leistung der Aufgabe zu optimieren. Dadurch wird die CPU-Auslastung auf dem geschützten Gerät reduziert. Sie können die Untersuchung von Archiven einschränken, die maximale Größe der Objekte festlegen, die untersucht werden können, und die maximale Dauer der Objektuntersuchung festlegen. Kaspersky Endpoint Security ermöglicht es außerdem, Dateien bestimmter Formate von der Untersuchung auszuschließen: Archive, E-Mail-Datenbanken, Textdateien und E-Mail-Nachrichten im Nur-Text-Format.

So konfigurieren Sie die Untersuchung von Dateien über die Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Wählen Sie in der Aufgabenliste die Aufgabe „Untersuchung von Containern in Kaspersky Endpoint Security“ aus und klicken Sie auf den Namen der Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Konfigurieren Sie unter **Untersuchungseinstellungen** die Untersuchung von Dateien:

   - **Archive untersuchen**. Untersucht Archive der Formate ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE und mehr. Die Anwendung durchsucht Archive nicht nur nach Dateiendung, sondern auch nach Format. Bei der Untersuchung von Archiven entpackt die Anwendung diese rekursiv. Dadurch können Bedrohungen in verschachtelten Archiven (d. h. Archive in Archiven) erkannt werden. Die Untersuchung ist standardmäßig deaktiviert.
   - **SFX-Archive untersuchen**. Untersuchung von selbstentpackenden Archiven, die ein ausführbares Entpackungsmodul enthalten. Die Untersuchung ist standardmäßig deaktiviert.
   - **E-Mail-Datenbanken untersuchen**. Untersuchung von E-Mail-Datenbanken für Microsoft Outlook, Outlook Express, The Bat! und andere E-Mail-Programme. Die Untersuchung ist standardmäßig deaktiviert.

- **Dateien in E-Mail-Formaten untersuchen**. E-Mail-Nachrichten im Nur-Text-Format untersuchen. Die Untersuchung ist standardmäßig deaktiviert.

- **Datei überspringen, wenn Untersuchung länger dauert als (Sek.)**. Maximale Untersuchungsdauer (in Sekunden) eines Objekts. Die Anwendung stellt die Untersuchung eines Objekts ein, wenn sie länger dauert als durch diese Einstellung festgelegt. Standardmäßig versucht das Programm, ein Objekt innerhalb einer Minute zu untersuchen.

- **Dateien überspringen, wenn größer als (MB)**. Maximale Größe des zu untersuchenden Objekts (in Megabyte). Wenn die Größe des zu untersuchenden Objekts den angegebenen Wert überschreitet, überspringt die Anwendung das Objekt während der Untersuchung.

- **Dateien überspringen, wenn größer als (MB)**. Aufgeschobener Start von Untersuchungsaufgaben, wenn bereits eine Untersuchungsaufgabe ausgeführt wird. Kaspersky Endpoint Security reiht neue Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Beispiel: Das Programm hat nach Zeitplan eine vollständige Untersuchungsaufgabe gestartet. Wenn ein Benutzer versucht, eine schnelle Untersuchung über die Programmoberfläche zu starten, stellt Kaspersky Endpoint Security diese Aufgabe zur schnellen Untersuchung in die Warteschlange und startet diese Aufgabe automatisch, nachdem die vollständige Untersuchungsaufgabe abgeschlossen wurde.

5. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Untersuchung von Dateien über die Befehlszeile

1. Führen Sie den folgenden Befehl aus:

```
kesl --set-settings <task ID|name> ScanArchived=<Yes|No> ScanSfxArchived=<Yes|No> ScanMailBases=<Yes|No>
ScanPlainMail=<Yes|No> SkipPlainTextFiles=<Yes|No> SkipDatabaseJournals=<Yes|No> SizeLimit=<object size (MB)>
TimeLimit=<scan time (sec)> QueueScanTasks=<Yes|No>
```

   wobei:

   - `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

   - `<object size (MB)>` ist die maximale Größe eines zu untersuchenden Objekts (in Megabyte). Wenn die Größe des zu untersuchenden Objekts den angegebenen Wert überschreitet, überspringt die Anwendung das Objekt während der Untersuchung. Der Standardwert ist: `0`.

   - `<scan time (sec)>` ist die maximale Untersuchungsdauer für ein Objekt (in Sekunden). Die Anwendung stellt die Untersuchung eines Objekts ein, wenn sie länger dauert als durch diese Einstellung festgelegt. Der Standardwert ist: `0`.

2. Sie können die Einstellungen auch mithilfe einer Konfigurationsdatei anpassen:

   a. Geben Sie die Aufgabeneinstellungen in eine Konfigurationsdatei aus, indem Sie den folgenden Befehl ausführen:

```
kesl-control --get-settings <task ID|name> [--json]
```

   b. Öffnen Sie die Konfigurationsdatei zum Bearbeiten.

   c. Fügen Sie dieser Datei die folgenden Einstellungen der Aufgabe *Untersuchung von Containern* hinzu, die für Objekte in Containern und Images gelten: `ScanArchived`, `ScanSfxArchived`, `ScanMailBases`, `ScanPlainMail`, `SizeLimit`, `TimeLimit`, `QueueScanTasks`.

d. Speichern Sie die Änderungen in der Konfigurationsdatei.

e. Importieren Sie die Einstellungen aus der Konfigurationsdatei mithilfe des folgenden Befehls in die Aufgabe:

```
kesl-control --set-settings <task ID|name> --file <path> [--json]
```

wobei:

- `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--file <path>` ist der vollständige Pfad zur Konfigurationsdatei, aus der Sie die Aufgabeneinstellungen importieren möchten.
- `--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 Anwendung, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Alle Werte der in der Datei definierten Aufgabeneinstellungen werden in die App importiert.

So wählen Sie eine Aktion aus, die beim Fund eines infizierten Objekts für einen Container ausgeführt werden soll

Wenn in einem Container ein infiziertes Objekt gefunden wird, kann Kaspersky Endpoint Security den Container sofort anhalten, keine Aktion ausführen oder den Container anhalten, wenn die Desinfektion des Objekts oder die Beseitigung der Bedrohung nicht möglich ist. Sie können die Aktion auswählen, die Kaspersky Endpoint Security mit dem Container ausführt, wenn ein infiziertes Objekt im Rahmen der Echtzeit-Untersuchung durch die Komponente *Container-Überwachung* oder im Rahmen einer Aufgabe zur *Untersuchung von Containern* bei Bedarf gefunden wird.

Wenn im Container-Image ein infiziertes Objekt gefunden wird, kann Kaspersky Endpoint Security das Image löschen oder keine Aktion mit dem Image ausführen. Sie können die Aktion auswählen, die Kaspersky Endpoint Security mit dem Container-Image ausführt, wenn ein infiziertes Objekt im Rahmen einer Aufgabe zur *Untersuchung von Containern* bei Bedarf gefunden wird.

So wählen Sie in der Web Console eine Aktion der Container-Überwachung beim Erkennen einer Bedrohung aus

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

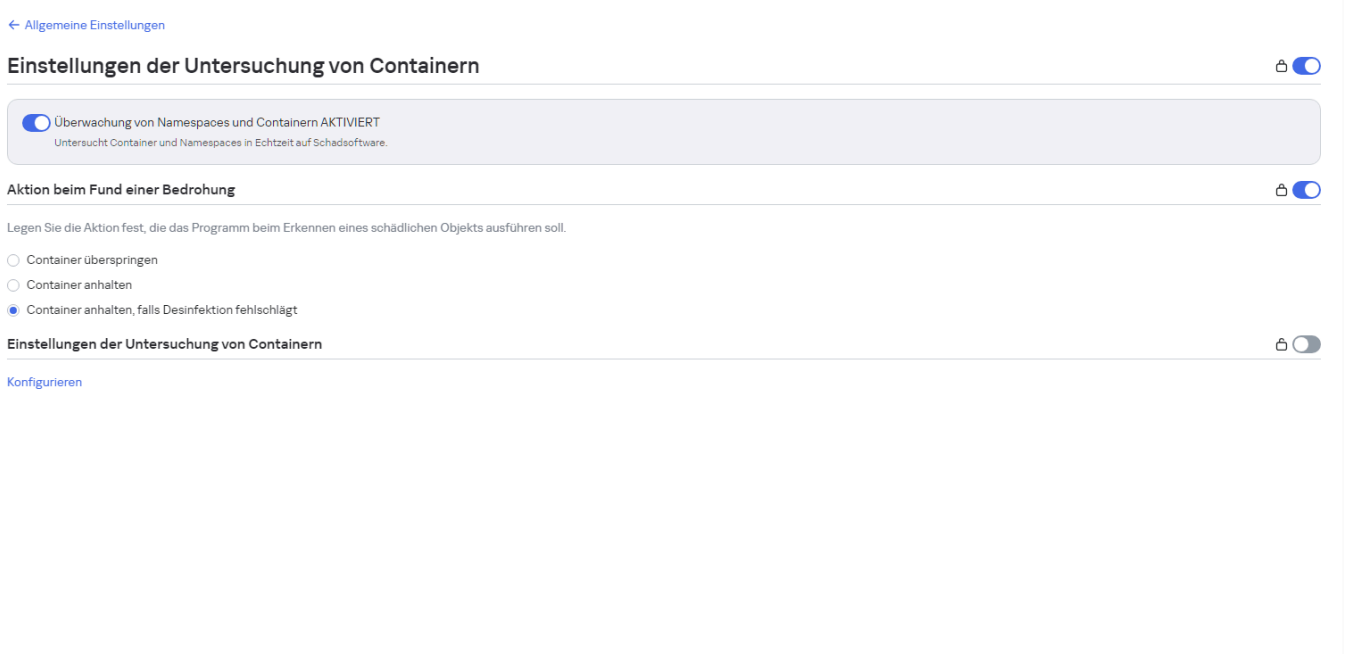
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Einstellungen der Untersuchung von Containern**.
5. Stellen Sie sicher, dass sich der Umschalter für die Komponente "Container-Überwachung" in der Position **Überwachung von Namespaces und Containern AKTIVIERT** befindet.

6. Wählen Sie unter **Aktion beim Fund einer Bedrohung** die Aktion aus, die das Programm ausführen soll, wenn in einem Container ein infiziertes Objekt gefunden wird:

   - **Container überspringen**. Wenn in einem Container ein infiziertes Objekt erkannt wird, führt das Programm keine Aktionen mit dem Container durch.
   - **Container anhalten**. Wenn in einem Container ein infiziertes Objekt erkannt wird, hält das Programm den Container an.
   - **Container anhalten, falls Desinfektion fehlschlägt** (Standardeinstellung). Wenn in einem Container ein infiziertes Objekt erkannt wird, versucht das Programm, das infizierte Objekt zu desinfizieren. Wenn ein infiziertes Objekt nicht desinfiziert werden konnte, hält das Programm den Container an.

   > 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 empfohlen, den Vorgang **Container anhalten** auszuwählen.

7. Speichern Sie die vorgenommenen Änderungen.



Einstellungen der Untersuchung von Containern

So wählen Sie in der Befehlszeile eine Aktion der Container-Überwachung beim Erkennen einer Bedrohung aus

1. Führen Sie den folgenden Befehl aus:

```
kesl-control --set-container-settings OnAccessContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>
```

> Diese Einstellung kann nur konfiguriert werden, wenn das Programm mit einer Lizenz, die diese Funktion unterstützt, verwendet wird.

2. Um die aktuellen Werte der Einstellungen für die Untersuchung von Containern zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings container-settings
```

So wählen Sie in der Web Console eine Aktion der Untersuchung von Containern beim Erkennen einer Bedrohung aus

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Wählen Sie in der Aufgabenliste die Aufgabe „Untersuchung von Containern in Kaspersky Endpoint Security“ aus und klicken Sie auf den Namen der Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wählen Sie unter **Erweiterte Untersuchungseinstellungen → Einstellungen der Untersuchung von Containern → Aktion beim Fund einer Bedrohung** die Aktion aus, die das Programm ausführen soll, wenn ein infiziertes Objekt in einem Container erkannt wird:

   - **Container überspringen**. Wenn in einem Container ein infiziertes Objekt erkannt wird, führt das Programm keine Aktionen mit dem Container durch.
   - **Container anhalten**. Wenn in einem Container ein infiziertes Objekt erkannt wird, hält das Programm den Container an.
   - **Container anhalten, falls Desinfektion fehlschlägt** (Standardeinstellung). Wenn in einem Container ein infiziertes Objekt erkannt wird, versucht das Programm, das infizierte Objekt zu desinfizieren. Wenn ein infiziertes Objekt nicht desinfiziert werden konnte, hält das Programm den Container an.

     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 empfohlen, den Vorgang **Container anhalten** auszuwählen.

5. Wählen Sie unter **Erweiterte Untersuchungseinstellungen → Image-Untersuchungseinstellungen → Aktion beim Fund einer Bedrohung** die Aktion aus, die das Programm ausführen soll, wenn ein infiziertes Objekt in einem Container erkannt wird:

   - **Image überspringen** (Standardeinstellung). Wenn im Image ein infiziertes Objekt erkannt wird, führt das Programm keine Aktionen mit dem Image durch.
   - **Image löschen** (nicht empfohlen). Wenn im Image ein infiziertes Objekt erkannt wird, löscht das Programm das Image. Alle Abhängigkeiten werden ebenfalls gelöscht. Laufende Container werden angehalten und anschließend gelöscht.

6. Speichern Sie die vorgenommenen Änderungen.

So wählen Sie in der Befehlszeile eine Aktion der Untersuchung von Containern beim Erkennen einer Bedrohung aus

1. Führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings <task ID|name> ContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>
ImageAction=<Skip|Delete>
```

Dabei ist `<task ID|name>` die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

> 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 empfohlen, den Vorgang `StopContainer` auszuwählen.

2. Sie können die Aktion auch mithilfe einer Konfigurationsdatei festlegen:

   a. Geben Sie die Aufgabeneinstellungen in eine Konfigurationsdatei aus, indem Sie den folgenden Befehl ausführen:

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. Öffnen Sie die Konfigurationsdatei zum Bearbeiten.

   c. Fügen Sie die folgenden Einstellungen der Aufgabe *Untersuchung von Containern* zur Datei hinzu:

   - `ContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>` – Aktion, die für einen Container ausgeführt werden soll, wenn ein infiziertes Objekt erkannt wird. Der Standardwert ist: `StopContainerIfFailed`.
   - `ImageAction=<Skip|Delete>` – Aktion, die für ein Container-Image ausgeführt werden soll, wenn ein infiziertes Objekt erkannt wird. Der Standardwert ist: `Skip`.

   d. Speichern Sie die Änderungen in der Konfigurationsdatei.

   e. Importieren Sie die Einstellungen aus der Konfigurationsdatei mithilfe des folgenden Befehls in die Aufgabe:

   ```
   kesl-control --set-settings <task ID|name> --file <path> [--json]
   ```

   Wobei gilt:

   - `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
   - `--file <path>` ist der vollständige Pfad zur Konfigurationsdatei, aus der Sie die Aufgabeneinstellungen importieren möchten.
   - `--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 Anwendung, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Alle Werte der in der Datei definierten Aufgabeneinstellungen werden in die App importiert.

So führen Sie eine benutzerdefinierte Untersuchung von Containern und Images aus

Um die Aufgabe „Benutzerdefinierte Untersuchung von Containern“ über die Befehlszeile zu starten, führen Sie den folgenden Befehl aus:

```
kesl-control --scan-container <id|name[:tag]>
```

wobei `<id|name[:tag]>` der Name oder die ID des Containers oder Images ist. Sie können Masken verwenden, um mehrere Objekte zu untersuchen.

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.

```
Beispiel für die Untersuchung eines Containers namens my_container
```

```
kesl-control --scan-container my_container
```

```
Beispiel für eine Untersuchung von Images, die für ein Image mit dem Namen my_image ausgeführt wird (alle Tags)
```

```
kesl-control --scan-container my_image*
```

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Untersuchung von Wechseldatenträgern

Kaspersky Endpoint Security untersucht alle Dateien, die Sie ausführen oder kopieren, selbst wenn sich die Datei auf einem Wechseldatenträger befindet. Das Programm untersucht Dateien auf CDs, DVDs, Blu-ray-Discs, Flash-Laufwerken (einschließlich USB-Modems), externen Festplatten und Disketten. Die Untersuchung von Wechseldatenträgern ist standardmäßig deaktiviert.

Funktionsweise der Untersuchung von Wechseldatenträgern

Wenn ein Wechseldatenträger angeschlossen wird, erstellt und startet das Programm automatisch die folgenden Untersuchungsaufgaben mit den Standardeinstellungen: *Untersuchung wichtiger Bereiche* für die schnelle Untersuchung und *Schadsoftware-Untersuchung* für die genaue Untersuchung. Diese Aufgaben können nicht angehalten werden. Wenn auf dem Wechseldatenträger eine Bedrohung erkannt wird, versucht Kaspersky Endpoint Security, das infizierte Objekt zu desinfizieren. Wenn eine Desinfektion nicht möglich ist, löscht das Programm das infizierte Objekt. Nach Abschluss der Untersuchung löscht das Programm diese Aufgaben automatisch.

Untersuchungstypen

- **Schnelle Untersuchung**. Kaspersky Endpoint Security untersucht nur Dateien mit den angegebenen Erweiterungen und entpackt keine zusammengesetzten Objekte. Das Programm führt eine schnelle Untersuchung mit den Standardeinstellungen der Aufgabe *Untersuchung wichtiger Bereiche* durch.
- **Genaue Untersuchung**. Kaspersky Endpoint Security untersucht alle Dateien auf Wechseldatenträgern. Das Programm führt eine genaue Untersuchung mit den Standardeinstellungen der Aufgabe *Schadsoftware-Untersuchung* durch.

So wählen Sie in der Web Console einen Typ für die Untersuchung von Wechseldatenträgern aus

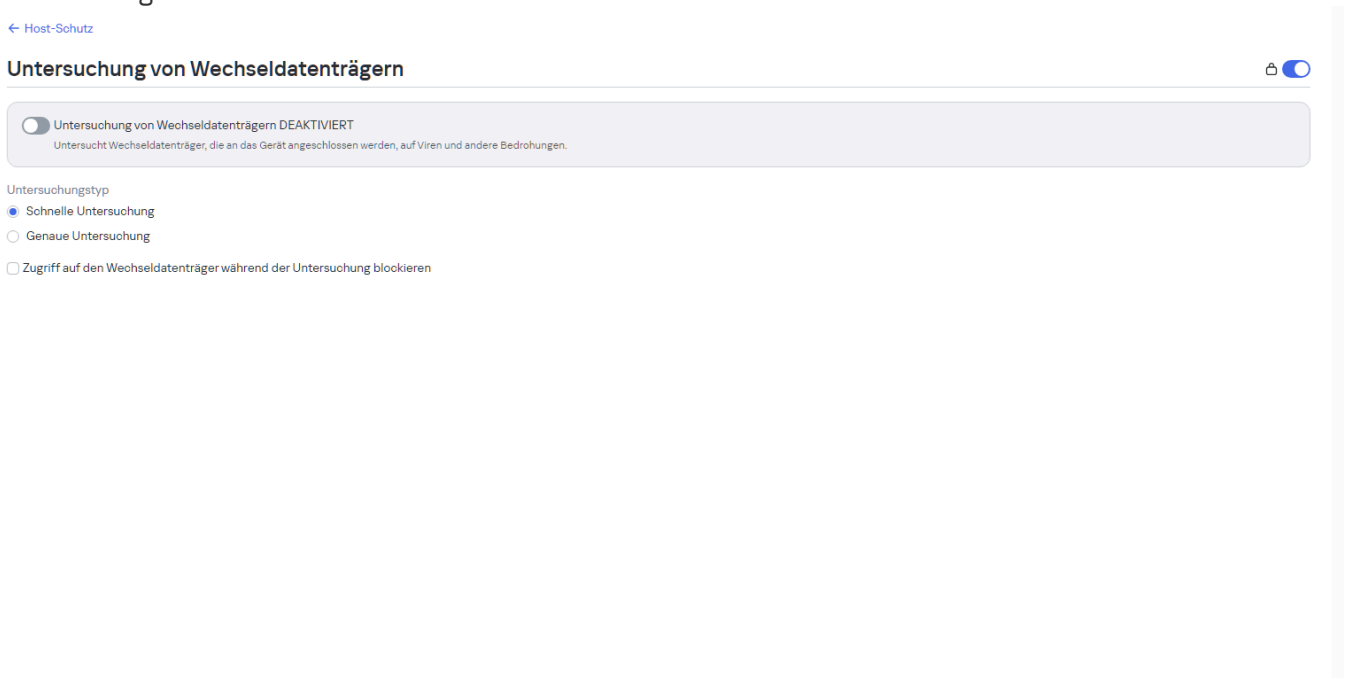
1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Untersuchung von Wechseldatenträgern**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **Untersuchung von Wechseldatenträgern AKTIVIERT** befindet.
6. Wählen Sie unter **Untersuchungstyp** den Typ der Untersuchung von Wechseldatenträgern aus: **Schnelle Untersuchung** oder **Genaue Untersuchung**.
7. Aktivieren Sie bei Bedarf das Kontrollkästchen **Zugriff auf Dateien während der Untersuchung blockieren**.

   Durch das Blockieren des Zugriffs auf Dateien wird verhindert, dass ein Benutzer während der Untersuchung Malware ausführt.

Während der Untersuchung von Bootsektoren blockiert das Programm keine Dateien.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Untersuchung von Wechseldatenträgern

So wählen Sie in der Befehlszeile einen Typ für die Untersuchung von Wechseldatenträgern aus

1. Wählen Sie den Typ der Untersuchung aus, die beim Anschließen von Wechseldatenträgern ausgeführt werden soll:

```
kesl-control --set-settings 16 ScanRemovableDrives=<DetailedScan|QuickScan|NoScan> BlockDuringScan=<Yes|No>
```

2. Wählen Sie den Typ der Untersuchung aus, die beim Einlegen von CD-/DVD-Laufwerken oder Blu-ray-Discs ausgeführt werden soll:

```
kesl-control --set-settings 16 ScanOpticalDrives=<DetailedScan|QuickScan|NoScan> BlockDuringScan=<Yes|No>
```

3. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 16
```

Symbole

Befehlsoptionen

Parameter	Description
`ScanRemovableDrives`	Typ der Untersuchung, die beim Anschließen von Wechseldatenträgern ausgeführt werden soll: • `DetailedScan`. Genaue Untersuchung. • `QuickScan`. Schnelle Untersuchung. • `NoScan` (Standardeinstellung). Das Programm führt keine Untersuchung durch.

Parameter	Description
`ScanOpticalDrives`	Typ der Untersuchung, die beim Einlegen von CD-/DVD-Laufwerken oder Blu-ray-Discs ausgeführt werden soll: • `DetailedScan`. Genaue Untersuchung. • `QuickScan`. Schnelle Untersuchung. • `NoScan` (Standardeinstellung). Das Programm führt keine Untersuchung durch.
`BlockDuringScan`	Den Zugriff auf Dateien auf dem verbundenen Datenträger während der Untersuchung blockieren. Standardmäßig blockiert das Programm den Zugriff auf Dateien nicht. Durch das Blockieren des Zugriffs auf Dateien wird verhindert, dass ein Benutzer während der Untersuchung Malware ausführt. Während der Untersuchung von Bootsektoren blockiert das Programm keine Dateien.

Verhaltensanalyse

Die Komponente „Verhaltensanalyse“ ermöglicht die Überwachung der Aktivität (Öffnen von Dateien, Herstellen von Verbindungen usw.) von Programmen, die den Computer oder Benutzerdaten gefährden können. Die Komponente überwacht das Verhalten von Programmen auf gefährliche Muster. Stimmt die Aktivität eines Programms mit einem dieser Muster überein, führt Kaspersky Endpoint Security die ausgewählte Reaktion aus. Diese Funktion von Kaspersky Endpoint Security bietet proaktiven Schutz für den Computer.

Für eine optimale Leistung der Komponente „Verhaltensanalyse“ wird empfohlen, die Komponente Schutz vor Web-Bedrohungen zu aktivieren.

Funktionsweise der Verhaltensanalyse

1. **Das Programm überwacht Ereignisse im Betriebssystem**

   Das Programm empfängt einen Telemetriedatenstrom, der aus Ereignissen besteht: Erstellen und Beenden von Prozessen, geöffnete Dateien, hergestellte Verbindungen usw. Außerdem reichert das Programm Ereignisse mit relevanten Metadaten an (Prozessname, PID, IP-Adresse usw.).

2. **Das Programm vergleicht den Telemetriedatenstrom mit Mustern für gefährliches Verhalten**

   Wenn die Aktionen eines Drittanbieter-Programms einem Muster für gefährliches Verhalten entsprechen, führt Kaspersky Endpoint Security eine Aktion zur Reaktion auf Bedrohungen aus (beispielsweise kann das Drittanbieter-Programm beendet werden).

3. **Das Programm sendet Telemetriedaten an KSN**

   Das Programm filtert Ereignisse und sendet sie zur weiteren Analyse an KSN.

Verhaltensanalyse konfigurieren

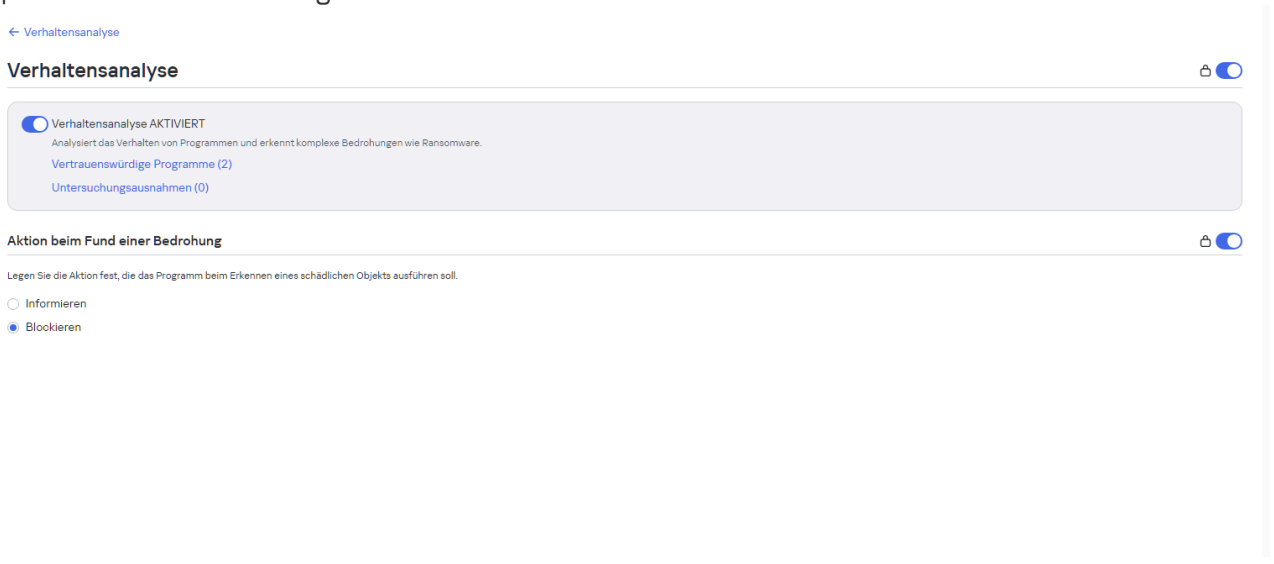
1. **Wählen Sie in den Einstellungen der Verhaltensanalyse die Aktion Informieren aus**

Die Komponente „Verhaltensanalyse“ ist standardmäßig aktiviert. In den Einstellungen der Verhaltensanalyse wird empfohlen, **Informieren** als Aktion beim Erkennen einer Bedrohung auszuwählen und zu überprüfen, ob die installierten Programme ordnungsgemäß funktionieren. Kaspersky Endpoint Security erlaubt alle Programmaktivitäten und protokolliert die Ausführung der Komponente.

So wählen Sie in der Web Console eine Aktion bei Erkennung von Malware-Aktivität aus

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Verhaltensanalyse** → **Verhaltensanalyse**.
5. Wählen Sie die entsprechende Aktion im Block **Aktion beim Fund einer Bedrohung**:
   - **Informieren**. Wenn schädliche Aktivität erkannt wird, beendet Kaspersky Endpoint Security dieses Programm nicht, sondern protokolliert lediglich ein Ereignis zur Erkennung schädlicher Aktivität im Ereignisprotokoll.
   - **Blockieren**. Wenn schädliche Aktivität erkannt wird, beendet Kaspersky Endpoint Security den Prozess des Programms, das die schädliche Aktivität ausführt, und protokolliert Informationen über die erkannte schädliche Aktivität.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Verhaltensanalyse

So wählen Sie über die Befehlszeile eine Aktion bei Erkennung von Malware-Aktivität aus

1. Führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 20 TaskMode=<Block|Notify>
```

2. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 20
```

Symbole

Befehlsoptionen

Parameter	Description
`TaskMode`	Aktion bei Erkennung von Malware-Aktivität: • `Block` (Standardeinstellung). Wenn schädliche Aktivität erkannt wird, beendet Kaspersky Endpoint Security den Prozess des Programms, das die schädliche Aktivität ausführt, und protokolliert Informationen über die erkannte schädliche Aktivität. • `Notify`. Wenn schädliche Aktivität erkannt wird, beendet Kaspersky Endpoint Security dieses Programm nicht, sondern protokolliert lediglich ein Ereignis zur Erkennung schädlicher Aktivität im Ereignisprotokoll.

2 Statistiken zur Verhaltensanalyse sammeln

Sie können Statistiken zur Verhaltensanalyse über Berichte abrufen.

3 Programmleistung optimieren

Optimieren Sie nach der Analyse der gesammelten Informationen die Programmleistung und fügen Sie Ausnahmen hinzu.

4 Wählen Sie in den Einstellungen der Verhaltensanalyse die Aktion Blockieren aus

Aktivieren Sie die Blockierung schädlicher Aktivitäten von Programmen. Danach beendet Kaspersky Endpoint Security die Prozesse von Programmen, die schädliche Aktivitäten ausführen.

Besonderheiten und Einschränkungen

- Damit die Komponente „Verhaltensanalyse“ ordnungsgemäß funktioniert, wenn Kaspersky Endpoint Security in die Lösungen Kaspersky Managed Detection and Response und Kaspersky Anti Targeted Attack Platform integriert ist, stellen Sie sicher, dass auditd in den Konfigurationsdateien auf den Modus ohne Konfigurationsblockierung `enabled 1` gesetzt ist.

Exploit-Prävention

Die Exploit-Prävention überwacht Code, der Schwachstellen auf Ihrem Gerät ausnutzt, um Administratorrechte zu erlangen oder schädliche Aktionen auszuführen.

Damit die Komponente „Exploit-Prävention“ funktioniert, müssen die folgenden Komponenten aktiviert sein:

- Verhaltensanalyse
- Aktualisierbares Kernel-Modul

Die Komponente ist für Geräte mit Elbrus-CPU nicht verfügbar.

So funktioniert die Exploit-Prävention

1. **Das Programm überwacht Ereignisse im Betriebssystem**

   Das Programm empfängt einen Telemetriedatenstrom, der aus Ereignissen besteht: Erstellen und Beenden von Prozessen, geöffnete Dateien, hergestellte Verbindungen usw. Außerdem reichert das Programm Ereignisse mit relevanten Metadaten an (Prozessname, PID, IP-Adresse usw.).

2. **Das Programm vergleicht den Telemetriedatenstrom mit Mustern für gefährliches Verhalten**

   Wenn die Aktionen eines Drittanbieter-Programms einem Muster für gefährliches Verhalten entsprechen, führt Kaspersky Endpoint Security eine Aktion zur Reaktion auf Bedrohungen aus (beispielsweise kann das Drittanbieter-Programm beendet werden).

Konfigurieren der Exploit-Prävention

1. **Wählen Sie in den Einstellungen der Exploit-Prävention die Aktion „Informieren“ aus**

   Standardmäßig ist die Komponente „Exploit-Prävention“ deaktiviert. Wählen Sie in den Einstellungen der Exploit-Prävention **Informieren** als Aktion beim Erkennen einer Bedrohung aus und überprüfen Sie, ob die installierten Programme ordnungsgemäß funktionieren. Kaspersky Endpoint Security lässt alle Programmaktivitäten zu und protokolliert Informationen über erkannte Bedrohungen.

   So wählen Sie die Aktion beim Erkennen eines Exploits in der Web Console aus

   1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
   2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

      Das Eigenschaftenfenster der Richtlinie wird geöffnet.
   3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
   4. Gehen Sie zu **Host-Schutz** → **Verhaltensanalyse** → **Exploit-Prävention**.
   5. Verwenden Sie den Schalter **Exploit-Prävention**, um die Komponente zu aktivieren oder zu deaktivieren.
   6. Wählen Sie die entsprechende Aktion im Block **Aktion beim Fund einer Bedrohung**:

      - **Blockieren**. Wenn dieses Element ausgewählt ist und ein Exploit gefunden wird, blockiert Kaspersky Endpoint Security die Aktivitäten dieses Exploits und erstellt einen Berichtseintrag, der Informationen über diesen Exploit enthält.
      - **Informieren**. Wenn dieses Element ausgewählt ist und ein Exploit gefunden wird, erstellt Kaspersky Endpoint Security einen Berichtseintrag, der Informationen über den Exploit enthält, und fügt Informationen über diesen Exploit zur Liste der aktiven Bedrohungen hinzu.
   7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So wählen Sie die Aktion beim Erkennen einer Bedrohung in der Befehlszeile aus

1. Um die Exploit-Prävention zu aktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 20 UseAEP=Yes
```

2. Wählen Sie eine Aktion beim Erkennen eines Exploits aus:

```
kesl-control --set-settings 20 AEPMode=<Block|Notify>
```

3. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 20
```

Symbole

Befehlsoptionen

Parameter	Description
`UseAEP`	Aktivieren der Komponente: • `Yes` aktiviert die Exploit-Prävention. • `No` (Standardwert) – Die Exploit-Prävention ist deaktiviert.
`AEPMode`	Aktion beim Erkennen eines Exploits: • `Block` (Standardeinstellung). Kaspersky Endpoint Security blockiert die Aktivitäten dieses Exploits und erstellt einen Protokolleintrag mit Informationen über diesen Exploit. • `Notify`. Wenn Kaspersky Endpoint Security einen Exploit erkennt, erstellt das Programm einen Protokolleintrag mit Informationen über den Exploit und fügt Informationen über diesen Exploit zur Liste der aktiven Bedrohungen hinzu.

2 Statistiken zur Exploit-Prävention erfassen

Sie können Statistiken zur Exploit-Prävention mithilfe von Berichten abrufen.

3 Programmleistung optimieren

Optimieren Sie nach der Analyse der gesammelten Informationen die Leistung des Programms:

- Globale Ausnahmen hinzufügen
- Ausnahmen hinzufügen

4 Wählen Sie in den Einstellungen der Exploit-Prävention die Aktion „Blockieren“ aus

Aktivieren Sie die Blockierung bösartiger Aktivitäten von Programmen im Betriebssystem.

Schutz vor Verschlüsselung

Die Komponente „Schutz vor Verschlüsselung“ schützt vor Remote-Verschlüsselung, indem sie die Aktivitäten von Remote-Geräten in freigegebenen Netzwerkverzeichnissen des Computers analysiert. Schutz vor Verschlüsselung analysiert Dateien, die über die Protokolle NFS und SMB an den geschützten Computer übertragen werden.

Wenn die Aktivität mit einer Verhaltensstrom-Signatur übereinstimmt, die für externe Verschlüsselung typisch ist, blockiert Kaspersky Endpoint Security diese Aktivität oder informiert Sie darüber.

Funktionsweise von Schutz vor Verschlüsselung

1. **Das Programm fängt NFS- und SMB-Anfragen ab**

   Das Programm empfängt einen Strom von Telemetriedaten über die Erstellung und Änderung von Dateien, die über die Protokolle NFS und SMB übertragen werden.

2. **Das Programm vergleicht den Strom von Telemetriedaten mit Signaturdatenbanken.**

   Wenn die Aktionen des Drittanbieter-Programms denen von Ransomware entsprechen, führt Kaspersky Endpoint Security die ausgewählte Aktion beim Erkennen einer Bedrohung aus (z. B. das Blockieren der Verbindung zum Remote-Computer).

Schutz vor Verschlüsselung konfigurieren

1. **Schutzbereich konfigurieren**

   Standardmäßig untersucht das Programm alle freigegebenen Verzeichnisse. Wenn Sie nur ein einzelnes Verzeichnis untersuchen müssen (z. B. das Verzeichnis, in das Dateien automatisch aus einer externen Quelle heruntergeladen werden), können Sie nur dieses Verzeichnis als Schutzbereich festlegen. In anderen Fällen empfehlen wir, den Standardschutzbereich beizubehalten und Ausnahmen zu verwenden, um den Bereich gezielt anzupassen.

2. **Wählen Sie in den Einstellungen für den Schutz vor Verschlüsselung die Aktion „Informieren“ aus**

   Schutz vor Verschlüsselung ist standardmäßig deaktiviert. Wir empfehlen, den Schutz vor Verschlüsselung zu aktivieren, als Aktion beim Erkennen einer Bedrohung die Option **Informieren** auszuwählen und den Zugriff auf alle Unternehmensressourcen zu überprüfen. Kaspersky Endpoint Security erlaubt den Zugriff auf alle Ressourcen in freigegebenen Verzeichnissen und protokolliert Informationen über erkannte Bedrohungen.

3. **Statistiken für Schutz vor Verschlüsselung sammeln**

   Sie können Statistiken für Schutz vor Verschlüsselung mithilfe von Berichten abrufen.

4. **Programmleistung optimieren**

   Optimieren Sie nach der Analyse der gesammelten Informationen die Leistung des Programms:

   - Globale Ausnahmen hinzufügen.
   - Ausnahmen hinzufügen.

5. **Wählen Sie in den Einstellungen für den Schutz vor Verschlüsselung die Aktion „Verbindung blockieren“ aus**

   Aktivieren Sie die Blockierung des Netzwerkverkehrs von einem angreifenden Remote-Gerät.

Besonderheiten und Einschränkungen

- Die Komponente „Schutz vor Verschlüsselung“ funktioniert ordnungsgemäß mit den Protokollen SMB1, SMB2, SMB3, NFS3, TCP/UDP und IP. Die Protokolle NFS2 und NFS4 werden nicht unterstützt. Es wird empfohlen, Ihren Server so zu konfigurieren, dass die Protokolle NFS2 und NFS4 nicht zum Mounten von Ressourcen verwendet werden können.

- Damit die Komponente „Schutz vor Verschlüsselung“ ordnungsgemäß funktioniert, muss mindestens einer der Dienste (Samba oder NFS) im Betriebssystem installiert sein. Für den NFS-Dienst muss das Paket rpcbind installiert sein.

- Kaspersky Endpoint Security blockiert den Zugriff auf Netzwerkdateiressourcen erst dann, wenn die Aktivität eines Remote-Geräts als bösartig eingestuft wurde. Es wird daher mindestens eine Datei verschlüsselt, bevor die App eine bösartige Aktivität erkennt.

Aktion beim Fund bösartiger Verschlüsselung auswählen

Wenn bösartige Verschlüsselung erkannt wird, kann das Programm den Netzwerkverkehr eines entfernten angreifenden Geräts blockieren oder lediglich über den Fund bösartiger Verschlüsselung informieren.

Um den Netzwerkverkehr zu blockieren, erstellt Kaspersky Endpoint Security eine dynamische Firewall-Regel. Die Firewall blockiert vorübergehend den Netzwerkverkehr für das angreifende Gerät. Außerdem fügt das Programm das angreifende Gerät der Liste der blockierten Geräte hinzu. Blockierten Geräten wird der Zugriff auf freigegebene Netzwerkverzeichnisse verweigert.

Um den Administrator über den Fund bösartiger Verschlüsselung zu informieren, generiert das Programm ein Ereignis *Verschlüsselung erkannt*.

Standardmäßig blockiert das Programm den Netzwerkverkehr eines angreifenden Geräts für 60 Minuten. Nach Ablauf der Sperrzeit entfernt das Programm das gefährdete Gerät aus der Liste der blockierten Geräte, und der Zugriff des Geräts auf Netzwerkdateiressourcen wird automatisch wiederhergestellt.

Sie können lokal auf dem Computer des Benutzers die Liste der blockierten Geräte anzeigen und die Blockierung dieser Geräte manuell aufheben. Kaspersky Security Center verfügt über keine Tools zur Überwachung und Verwaltung blockierter Geräte, mit Ausnahme des Ereignisses *Verschlüsselung erkannt*.

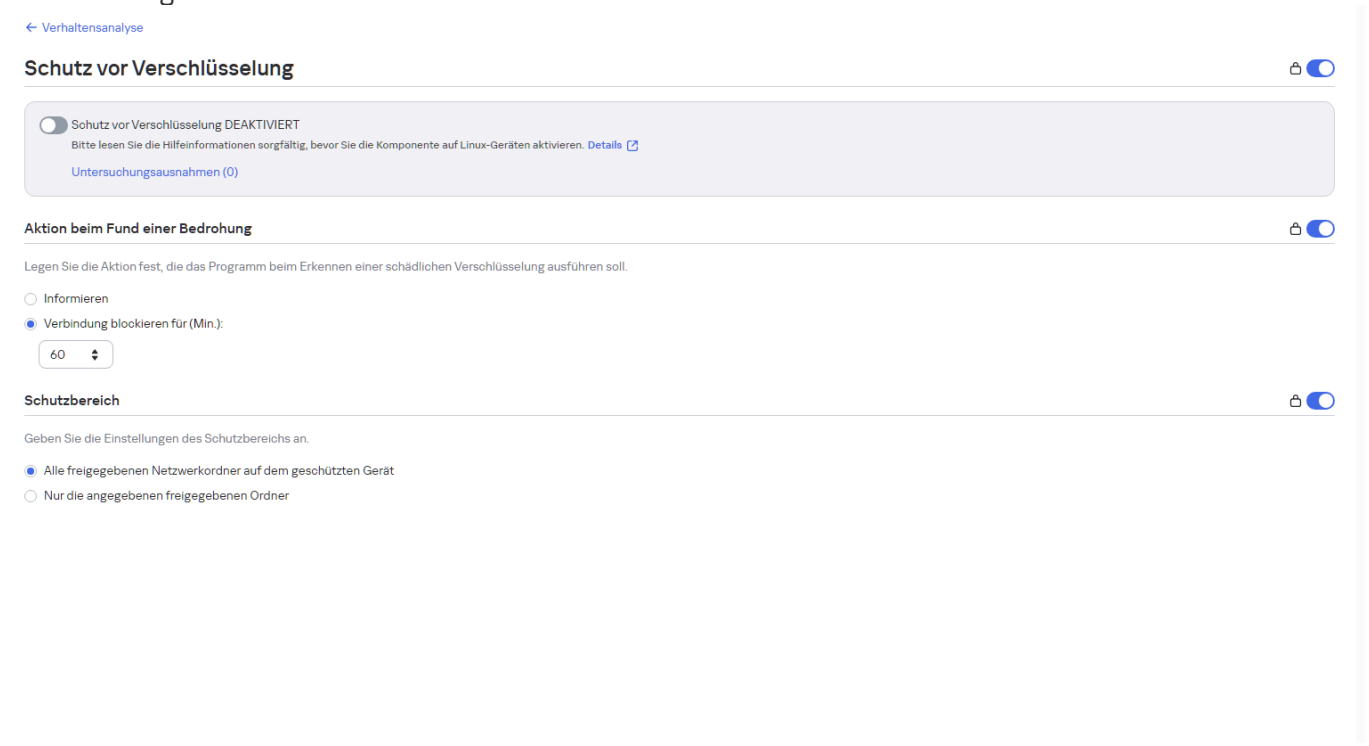
Aktionen beim Fund bösartiger Verschlüsselung in der Web Console konfigurieren

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Verhaltensanalyse** → **Schutz vor Verschlüsselung**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **Schutz vor Verschlüsselung AKTIVIERT** befindet.
6. Wählen Sie unter **Aktion beim Fund einer Bedrohung** die Aktion aus, die die App bei Erkennung einer Bedrohung ausführen soll: **Informieren** oder **Verbindung blockieren für (Min.)**.

7. Wenn **Verbindung blockieren für (Min.)** ausgewählt ist, legen Sie die Sperrzeit für das angreifende Gerät in Minuten fest. Standardmäßig wird das Gerät für 60 Minuten blockiert.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Schutz vor Verschlüsselung

Aktionen beim Fund bösartiger Verschlüsselung über die Befehlszeile konfigurieren

1. Führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 13 ActionOnDetect=<Block|Notify>
```

2. Wählen Sie die Sperrzeit für die Aktion `Block` aus.

```
kesl-control --set-settings 13 BlockTime=<Blocking period>
```

3. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 13
```

Symbole

Befehlsoptionen

Parameter	Description
`ActionOnDetect`	Aktion beim Erkennen externer Verschlüsselung: • `Block` (Standard) blockiert den Netzwerkverkehr für das angreifende Gerät und erstellt ein Ereignis *Verschlüsselung erkannt*. • `Notify` erstellt ein Ereignis *Verschlüsselung erkannt*, ohne den Netzwerkverkehr zu blockieren.
`BlockTime`	Sperrzeit für die angreifenden Geräte in Minuten.

So erstellen Sie einen Schutzbereich

Ein *Schutzbereich* ist eine Liste mit Pfaden zu freigegebenen Netzwerkverzeichnissen, in denen Kaspersky Endpoint Security die Dateiaktivität überwacht. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske. Standardmäßig identifiziert das Programm automatisch freigegebene Netzwerkverzeichnisse und überwacht die Dateiaktivität in diesen Verzeichnissen.

Bei Bedarf können Sie die Überwachung der Dateiaktivität auf schädliche Verschlüsselung auf eine Teilmenge von Verzeichnissen beschränken. 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.

Durch das Ausschließen eines Verzeichnisses aus dem Schutzbereich lässt sich die Anzahl der Fehlalarme reduzieren, wenn Ihr Unternehmen beim Austausch von Dateien über freigegebene Netzwerkverzeichnisse Datenverschlüsselung verwendet. Der Schutz vor Verschlüsselung kann beispielsweise Fehlalarme auslösen, wenn der Benutzer in einem freigegebenen Ordner mit Dateien mit der Erweiterung ENC arbeitet. Diese Aktivität gleicht einem Verhaltensmuster, das für externe Verschlüsselung charakteristisch ist. Wenn Sie zum Schutz von Daten verschlüsselte Dateien in einem freigegebenen Netzwerkverzeichnis haben, fügen Sie dieses Verzeichnis den Ausnahmen hinzu.

So erstellen Sie einen Schutzbereich in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Verhaltensanalyse** → **Schutz vor Verschlüsselung**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **Schutz vor Verschlüsselung AKTIVIERT** befindet.
6. Wählen Sie unter **Schutzbereich** den Punkt **Nur die angegebenen freigegebenen Ordner** auswählen.
7. Klicken Sie in der Liste der Verzeichnisse auf **Hinzufügen**.
8. Daraufhin wird ein Fenster geöffnet; wählen Sie in diesem Fenster den Typ des Dateisystems aus:
   - **Lokal**. Verzeichnisse auf der Festplatte, auf die ohne Netzwerkverbindung zugegriffen werden kann.
   - **Freigegeben**. Computerverzeichnisse, auf die über das Samba- (SMB) oder das NFS-Protokoll zugegriffen werden kann.
   - **Alle freigegebenen**. Alle Computerverzeichnisse, auf die über die Protokolle Samba und NFS zugegriffen wird.
9. Geben Sie für ein lokales Dateisystem einen Verzeichnispfad an (z. B. `/path/to/folder`).

10. Geben Sie Masken für Objekterweiterungen an (z. B. `*.txt`). Trennen Sie die Masken durch Kommas.

11. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So erstellen Sie einen Schutzbereich über die Befehlszeile

1. Führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 13 ScanScope.item_#.UseScanArea=Yes \
        [ScanScope.item_#.AreaDesc=<description of the area>] \
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>] \
        [ScanScope.item_#.Path=<path to the directory>]
```

2. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 13
```

Symbole

Befehlsoptionen

Parameter	Description
`ScanScope.item_#.UseScanArea=Yes`	Aktivieren des Schutzbereichs mit der Nummer `#`. Sie können einen Schutzbereich vorübergehend ausschließen, anstatt ihn zu löschen. Legen Sie dazu `ScanScope.item_#.UseScanArea=No` fest.
`ScanScope.item_#.AreaDesc`	Beschreibung des Schutzbereichs; enthält zusätzliche Informationen zum Schutzbereich `#`.
`ScanScope.item_#.AreaMask.item_#`	Einschränkungen des Schutzbereichs. Im Schutzbereich schützt die Anwendung nur Dateien, die mit Masken im Shell-Format angegeben wurden. Beispiel `ScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt.`
`ScanScope.item_#.Path`	Pfad zum Verzeichnis mit den geschützten Objekten. Mögliche Werte: • `AllShared` (Standardeinstellung). Alle Computerverzeichnisse, auf die über die Protokolle Samba und NFS zugegriffen wird. • `Shared:SMB`. Verzeichnisse, auf die über das Samba-Protokoll (SMB) zugegriffen werden kann. • `Shared:NFS`. Verzeichnisse, auf die über das NFS-Protokoll zugegriffen werden kann. • `<path to local directory>`. Verzeichnisse auf der Festplatte, auf die ohne Netzwerkverbindung zugegriffen werden kann. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

```
Beispiel für einen Schutzbereich, der nur das Verzeichnis /home enthält

kesl-control --set-settings 13 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

Schutz vor modifizierten USB-Geräten

Angreifer können Schwachstellen in der Firmware eines USB-Geräts (z. B. eines Flash-Laufwerks) ausnutzen und das Gerät so umprogrammieren, dass das Betriebssystem dieses Gerät beim Anschließen als Tastatur erkennt. Infolgedessen kann ein infiziertes USB-Gerät unter Ihrem Benutzerkonto Befehle ausführen, um beispielsweise Malware herunterzuladen.

Mit der Schutzkomponente Schutz vor BadUSB-Angriffen kann der Anschluss eines infizierten USB-Geräts verhindert werden.

Die Komponente ist für Geräte mit Elbrus-CPU nicht verfügbar.

Funktionsweise des Schutzes vor BadUSB-Angriffen

1. **Das Programm fordert Sie auf, das USB-Gerät zu autorisieren**

   Wenn ein USB-Gerät mit dem Gerät verbunden wird, fordert das Programm den Benutzer auf, einen vom Programm generierten Zahlencode einzugeben. Dieser Vorgang wird als *Autorisierung* bezeichnet.

2. **Der Benutzer gibt den Autorisierungscode ein**

   Der Benutzer kann den Code über das angeschlossene USB-Gerät selbst (Tastatur oder Barcode-Scanner) oder, falls vorhanden, über eine Bildschirmtastatur eingeben. Sie können den Code nicht über ein bereits angeschlossenes USB-Gerät eingeben.

3. **Das Programm erlaubt autorisierte USB-Geräte und blockiert nicht autorisierte USB-Geräte**

   Wenn der Zahlencode korrekt eingegeben wurde, speichert das Programm die Identifikationsparameter, d. h. die VID/PID des USB-Geräts und die Nummer des Ports, mit dem es verbunden ist, in der Liste der autorisierten USB-Geräte. Dieses USB-Gerät muss nicht erneut autorisiert werden, wenn es erneut angeschlossen oder das Betriebssystem neu gestartet wird.

   Wenn der numerische Code falsch eingegeben wird, generiert das Programm einen neuen Code. Sie können die maximale Anzahl der Versuche für die Eingabe des Zahlencodes konfigurieren. Wenn der Zahlencode mehrmals falsch eingegeben wird, sperrt das Programm Eingaben von diesem USB-Gerät für eine bestimmte Zeit. Nachdem die Sperrzeit für das USB-Gerät abgelaufen ist, können Sie weitere Versuche unternehmen, das USB-Gerät zu autorisieren. Sie können die Zeit festlegen, nach deren Ablauf Sie weitere Versuche zur Eingabe des Autorisierungscodes unternehmen können.

Wenn ein autorisiertes USB-Gerät an einen anderen USB-Port angeschlossen wird, verlangt das Programm, dass es erneut autorisiert wird.

Schutz vor BadUSB-Angriffen konfigurieren

1. **Schutz vor BadUSB-Angriffen aktivieren**

   Die Komponente "Schutz vor BadUSB-Angriffen" ist standardmäßig deaktiviert. Identifizieren Sie Geräte, auf die nicht vertrauenswürdige Personen physischen Zugriff erhalten können und die vor externen Angreifern geschützt werden müssen, und aktivieren Sie auf diesen Geräten die Komponente Schutz vor BadUSB-Angriffen. Nach der Aktivierung des Schutzes vor BadUSB-Angriffen erfordert das Programm die Autorisierung angeschlossener USB-Geräte, und Benutzer können nicht autorisierte USB-Geräte erst verwenden, nachdem diese autorisiert wurden. USB-Geräte, die vor der Aktivierung des Schutzes vor BadUSB-Angriffen angeschlossen wurden, gelten jedoch standardmäßig als autorisiert und erfordern keine Autorisierung.

   Schließen Sie keine nicht vertrauenswürdigen USB-Geräte an das Gerät an, bevor Sie den Schutz vor BadUSB-Angriffen aktiviert und konfiguriert haben.

2. **Schutz vor BadUSB-Angriffen konfigurieren**

   Konfigurieren Sie je nach Typ der angeschlossenen USB-Geräte (Tastaturen oder Barcode-Scanner), wie der Autorisierungscode angezeigt werden soll: als Barcode oder als Zahlencode (Standardeinstellung).

   Konfigurieren Sie bei Bedarf die Autorisierung von USB-Geräten:

   - Maximale Anzahl von Versuchen zur Eingabe des Autorisierungscodes
   - Blockierungsdauer des USB-Geräts bei Erreichen der maximalen Anzahl von Versuchen.

So konfigurieren Sie die Autorisierung von USB-Geräten

Wenn ein USB-Gerät, das vom Betriebssystem als Eingabegerät identifiziert wird, mit dem verwalteten Gerät verbunden wird, schlägt das Programm vor, das USB-Gerät mithilfe eines Zahlencodes oder Barcodes zu autorisieren. Wurde der Autorisierungscode falsch eingegeben, so generiert das Programm einen neuen Code. Wird der Autorisierungscode mehrmals falsch eingegeben oder das Autorisierungsfenster geschlossen, blockiert das Programm die Eingabe über dieses USB-Gerät. Nach Ablauf der Blockierungszeit für USB-Geräte oder wenn das Betriebssystem neu gestartet wird, fordert das Programm den Benutzer auf, die Autorisierung erneut durchzuführen.

In Kaspersky Endpoint Security können Sie die Autorisierung von USB-Geräten konfigurieren

- Maximale Anzahl der Autorisierungsversuche.
- Blockierungsdauer des USB-Geräts bei Erreichen der maximalen Anzahl von Versuchen.

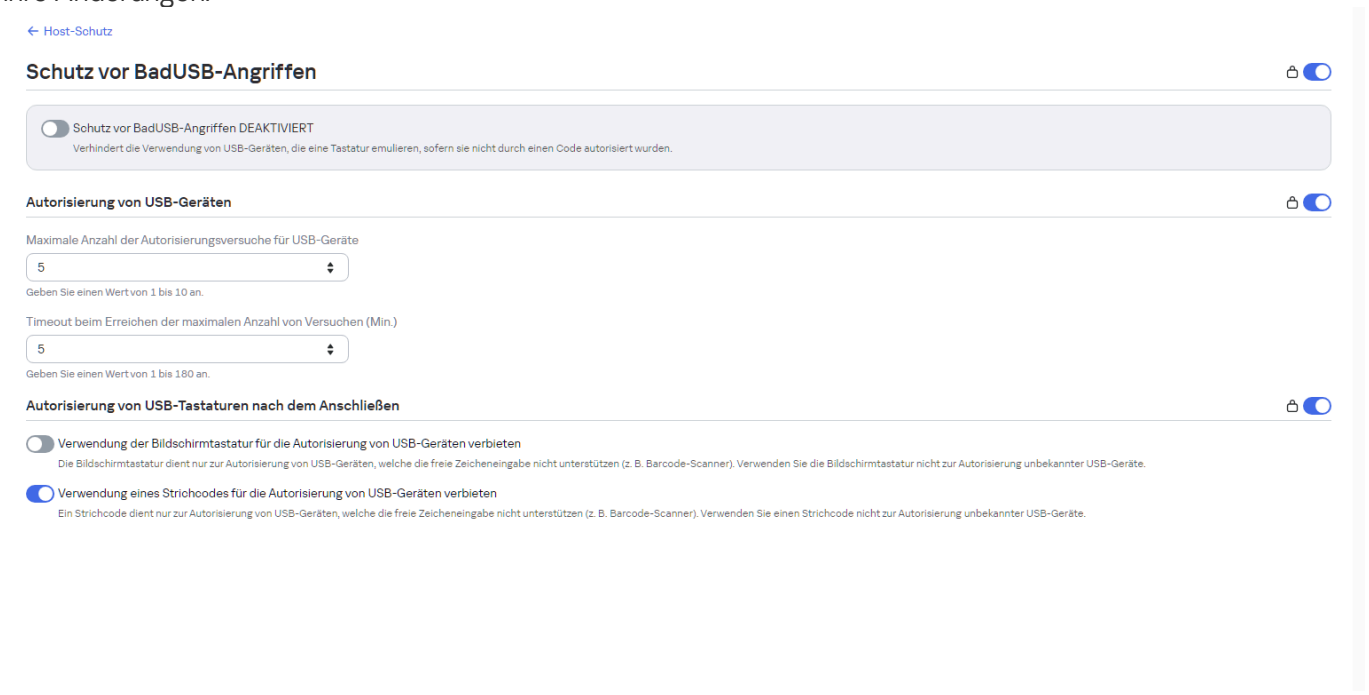
So konfigurieren Sie die Autorisierung von USB-Geräten in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Schutz vor BadUSB-Angriffen**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **Schutz vor BadUSB-Angriffen AKTIVIERT** befindet.
6. Konfigurieren Sie unter **Autorisierung von USB-Geräten** die Autorisierungseinstellungen:

   - **Maximale Anzahl der Autorisierungsversuche für USB-Geräte**. Das USB-Gerät wird automatisch gesperrt, wenn der Autorisierungscode zu oft falsch eingegeben wurde. Mögliche Werte: 1 bis 10. Wenn Sie beispielsweise 5 Versuche zur Eingabe des Autorisierungscodes erlauben, wird das USB-Gerät nach dem fünften erfolglosen Eingabeversuch durch die Anwendung blockiert. Kaspersky Endpoint Security zeigt den Zeitpunkt, an dem das USB-Gerät blockiert wurde. Nach Ablauf dieses Zeitraums haben Sie erneut fünf Versuche, den Autorisierungscode einzugeben.
   - **Timeout beim Erreichen der maximalen Anzahl von Versuchen (Min.)**. Die Dauer, für die ein USB-Gerät nach einer bestimmten Anzahl erfolgloser Eingabeversuche des Autorisierungscodes gesperrt wird. Die möglichen Werte liegen zwischen 1 und 180 (Minuten).

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Schutz vor modifizierten USB-Geräten

So konfigurieren Sie die Autorisierung von USB-Geräten über die Befehlszeile

1. Führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 37 MaxAuthAttempts=<number of attempts> TimeoutAfterAttempts=<timeout (minutes)>
```

2. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 37
```

Symbole

Befehlsoptionen

Parameter	Description
`MaxAuthAttempts`	Das USB-Gerät wird automatisch gesperrt, wenn der Autorisierungscode zu oft falsch eingegeben wurde. Mögliche Werte: 1 bis 10. Wenn Sie beispielsweise 5 Versuche zur Eingabe des Autorisierungscodes erlauben, wird das USB-Gerät nach dem fünften erfolglosen Eingabeversuch durch die Anwendung blockiert. Kaspersky Endpoint Security zeigt den Zeitpunkt, an dem das USB-Gerät blockiert wurde. Nach Ablauf dieses Zeitraums haben Sie erneut fünf Versuche, den Autorisierungscode einzugeben. Standardwert: 5.
`TimeoutAfterAttempts`	Die Dauer, für die ein USB-Gerät nach einer bestimmten Anzahl erfolgloser Eingabeversuche des Autorisierungscodes gesperrt wird. Die möglichen Werte liegen zwischen 1 und 180 (Minuten). Standardwert: 5 Minuten.

So erlauben Sie das Anschließen von USB-Geräten mithilfe der Bildschirmtastatur

Die Verwendung der Bildschirmtastatur ist nur für die Autorisierung von USB-Geräten vorgesehen, die die Eingabe beliebiger Zeichen nicht unterstützen (z. B. Barcode-Scanner). Es wird davon abgeraten, die Bildschirmtastatur für die Autorisierung unbekannter USB-Geräte zu verwenden. Standardmäßig ist die Verwendung der Bildschirmtastatur erlaubt.

Wir empfehlen, die Bildschirmtastatur nur zur Autorisierung von USB-Geräten zu verwenden, die dem Benutzer bekannt sind.

So aktivieren Sie die Autorisierung von USB-Geräten mithilfe der Bildschirmtastatur in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Schutz vor BadUSB-Angriffen**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **Schutz vor BadUSB-Angriffen AKTIVIERT** befindet.
6. Stellen Sie sicher, dass der Schalter **Verwendung der Bildschirmtastatur für die Autorisierung von USB-Geräten verbieten** deaktiviert ist. Der Schalter ist standardmäßig deaktiviert.
7. Um die Richtlinie auf Geräte anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren Sie die Autorisierung von USB-Geräten mithilfe der Bildschirmtastatur in der Befehlszeile

Führen Sie den Befehl aus:

```
kesl-control --set-settings 37 ProhibitOnScreenKeyboard=No
```

So erlauben Sie das Anschließen von USB-Geräten mithilfe des Barcode-Scanners

Wenn ein Barcode-Scanner an das Gerät angeschlossen wird, identifiziert die Komponente „Schutz vor BadUSB-Angriffen" diesen Scanner als Eingabegerät und fordert Sie auf, die Autorisierung durchzuführen. Um den Barcode-Scanner zu autorisieren, müssen Sie den Strichcode scannen, der auf dem Bildschirm angezeigt wird. Das Programm generiert einen Barcode im Code39-Format. Die meisten Barcode-Scanner und QR-Code-Scanner unterstützen dieses Format.

Das Programm unterstützt auch eine weitere Methode zur Autorisierung von Barcode-Scannern. Wenn Sie Geräte mit Touchscreen verwenden, können Sie über die Bildschirmtastatur einen Code eingeben. Dazu müssen Sie die Bildschirmtastatur genehmigen. Diese Methode ist beispielsweise bei stationären Barcode-Scannern praktisch, die in Kassengeräte eingebaut sind. Andere Autorisierungsmethoden für Barcode-Scanner sind nicht zulässig. Zur Autorisierung von USB-Geräten verwendet das Programm standardmäßig keinen Strichcode.

So aktivieren Sie die Autorisierung von USB-Geräten mithilfe des Barcode-Scanners in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Schutz vor BadUSB-Angriffen**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **Schutz vor BadUSB-Angriffen AKTIVIERT** befindet.
6. Deaktivieren Sie den Umschalter **Verwendung eines Strichcodes für die Autorisierung von USB-Geräten verbieten**.
7. Um die Richtlinie auf Geräte anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren Sie die Autorisierung von USB-Geräten mithilfe des Barcode-Scanners über die Befehlszeile

Führen Sie den Befehl aus:

```
kesl-control --set-settings 37 ProhibitBarcodeScanner=No
```

Schutz von Verbindungen und Kommunikation über das Netzwerk

Schutz vor E-Mail-Bedrohungen

Die Komponente "Schutz vor E-Mail-Bedrohungen" untersucht ein- und ausgehende E-Mail-Anhänge auf Viren und andere Bedrohungen. Diese Komponente schützt das Gerät mithilfe von Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und heuristischer Analyse.

Der Schutz vor E-Mail-Bedrohungen kann sowohl eingehende als auch ausgehende Nachrichten untersuchen. Das Programm unterstützt POP3, SMTP und IMAP in den folgenden E-Mail-Clients: Das Programm unterstützt außerdem erweiterte Versionen der Protokolle: POP3S, SMTPS und IMAPS.

Wenn ein Mail-Client in einem Browser geöffnet ist, untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ die Nachrichten nicht.

Damit der Schutz vor E-Mail-Bedrohungen funktioniert, müssen in den Netzwerkeinstellungen die Netzwerkports 25, 110, 143, 465, 587, 993 und 995 überwacht werden. Diese Netzwerkports sind standardmäßig in der Liste der überwachten Ports enthalten. Das Entfernen dieser Ports aus der Liste kann die Funktion der Komponente beeinträchtigen.

Die Komponente "Schutz vor E-Mail-Bedrohungen" ist standardmäßig aktiviert.

Funktionsweise des Schutzes vor E-Mail-Bedrohungen

Bei der Installation von Kaspersky Endpoint Security fügt das Programm ein selbstsigniertes Zertifikat hinzu: *Persönliches Root-Zertifikat von Kaspersky Anti-Virus*. Das Programm speichert dieses Zertifikat im lokalen Zertifikatsspeicher für vertrauenswürdige Zertifikate (`/etc/ssl/certs`). Bei jedem Programmstart prüft es, ob das Zertifikat vorhanden ist. Wenn das Zertifikat gelöscht wurde, stellt das Programm es automatisch wieder her.

1. **Das Programm fängt den E-Mail-Datenverkehr ab**

   Kaspersky Endpoint Security überprüft die Verbindung über die Protokolle POP3, SMTP und IMAP.

2. **Das Programm untersucht eingehende und ausgehende Nachrichten**

   Der Schutz vor E-Mail-Bedrohungen untersucht den Datenverkehr mithilfe der folgenden Technologien:

   - Antiviren-Datenbanken.
   - Cloud-Dienste von Kaspersky Security Network.
   - Die Technologie der heuristischen Analyse ermöglicht die Erkennung von Bedrohungen, die noch nicht in den Kaspersky-Datenbanken erfasst sind.

3. **Das Programm schließt die Untersuchung ab**

   Wenn eine eingehende Nachricht im Anhang oder im Nachrichtentext eine Bedrohung enthält, führt Kaspersky Endpoint Security die Aktion beim Erkennen einer Bedrohung aus. Wenn in einer ausgehenden Nachricht eine Bedrohung erkannt wird, blockiert der Schutz vor E-Mail-Bedrohungen den Versand dieser Nachricht.

Schutz vor E-Mail-Bedrohungen konfigurieren

1. **Gruppe für die Testbereitstellung der Komponente festlegen**

   Stellen Sie eine kleine Gruppe von Geräten zusammen, auf denen Sie die Konfiguration der Komponente „Schutz vor E-Mail-Bedrohungen“ testen. Auf diese Weise können Sie sicherstellen, dass die Komponente korrekt konfiguriert ist, und den stabilen Betrieb des E-Mail-Clients gewährleisten, um mögliche Fehler zu vermeiden.

2. **Anhangsfilter konfigurieren**

   Standardmäßig bietet der von Kaspersky konfigurierte Filter des Schutzes vor E-Mail-Bedrohungen die empfohlene Schutzstufe. Wenn Sie spezielle Anforderungen an die E-Mail-Sicherheit haben, können Sie die Einstellungen des Anhangsfilters ändern.

3. **Untersuchung von Nachrichten konfigurieren**

   Konfigurieren Sie bei Bedarf die Untersuchung von E-Mail-Nachrichten entsprechend den Parametern Ihres Mailservers. Sie können beispielsweise die Größe der untersuchten Archive begrenzen, um die Belastung des Mailservers zu verringern.

4. **Überprüfen, ob der Schutz vor E-Mail-Bedrohungen korrekt funktioniert**

   Erstellen Sie eine Testnachricht mit einem schädlichen Anhang. Senden Sie die Nachricht an die ausgewählte Gerätegruppe und überprüfen Sie, ob der schädliche Inhalt der Nachricht gemäß den Komponenteneinstellungen verarbeitet wurde.

   Sie können auch überprüfen, ob das Programm das entsprechende *Bedrohung erkannt*-Ereignis generiert hat, indem Sie folgenden Befehl ausführen:

   ```
   kesl-control -E -q "TaskName == 'Mail_Monitoring'"
   ```

5. **Einstellungen für den Schutz vor E-Mail-Bedrohungen auf alle Geräte in der Organisation anwenden**

Besonderheiten und Einschränkungen

- Wenn der E-Mail-Client auf den geschützten Geräten keinen lokalen Speicher für vertrauenswürdige Zertifikate verwendet, fügen Sie das Zertifikat *Persönliches Root-Zertifikat von Kaspersky Anti-Virus* manuell zum Speicher für vertrauenswürdige Zertifikate des E-Mail-Clients hinzu. Weitere Informationen zum Hinzufügen eines Zertifikats finden Sie in der offiziellen Dokumentation Ihres E-Mail-Clients.

- Der Schutz vor E-Mail-Bedrohungen versucht nicht, schädliche Anhänge in ausgehenden E-Mails zu desinfizieren. Ausgehende Nachrichten mit schädlichen Anhängen werden entweder vollständig blockiert oder zugelassen.

Was ist zu tun, wenn eine E-Mail-Bedrohung erkannt wird

Wenn ein infiziertes Objekt im Anhang einer *ausgehenden Nachricht* erkannt wird, verhindert das Programm den Versand der Nachricht.

Wenn in einer *eingehenden Nachricht* ein infiziertes Objekt erkannt wird, kann das Programm versuchen, das Objekt zu desinfizieren und anschließend entweder das Objekt löschen oder den Zugriff auf das Objekt blockieren. Kaspersky Endpoint Security fügt außerdem Informationen über die ausgeführte Aktion zum Nachrichtenbetreff hinzu, z. B. *[Die Nachricht wurde verarbeitet.] <Nachrichtenbetreff>*.

Beim Konfigurieren des Schutzes vor E-Mail-Bedrohungen können Sie auswählen, welche Aktionen Kaspersky Endpoint Security ausführen soll, wenn in E-Mail-Nachrichten eine Bedrohung erkannt wird.

So konfigurieren Sie Aktionen beim Erkennen von Bedrohungen in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Kommunikations- und Web-Schutz** → **Schutz vor E-Mail-Bedrohungen**.

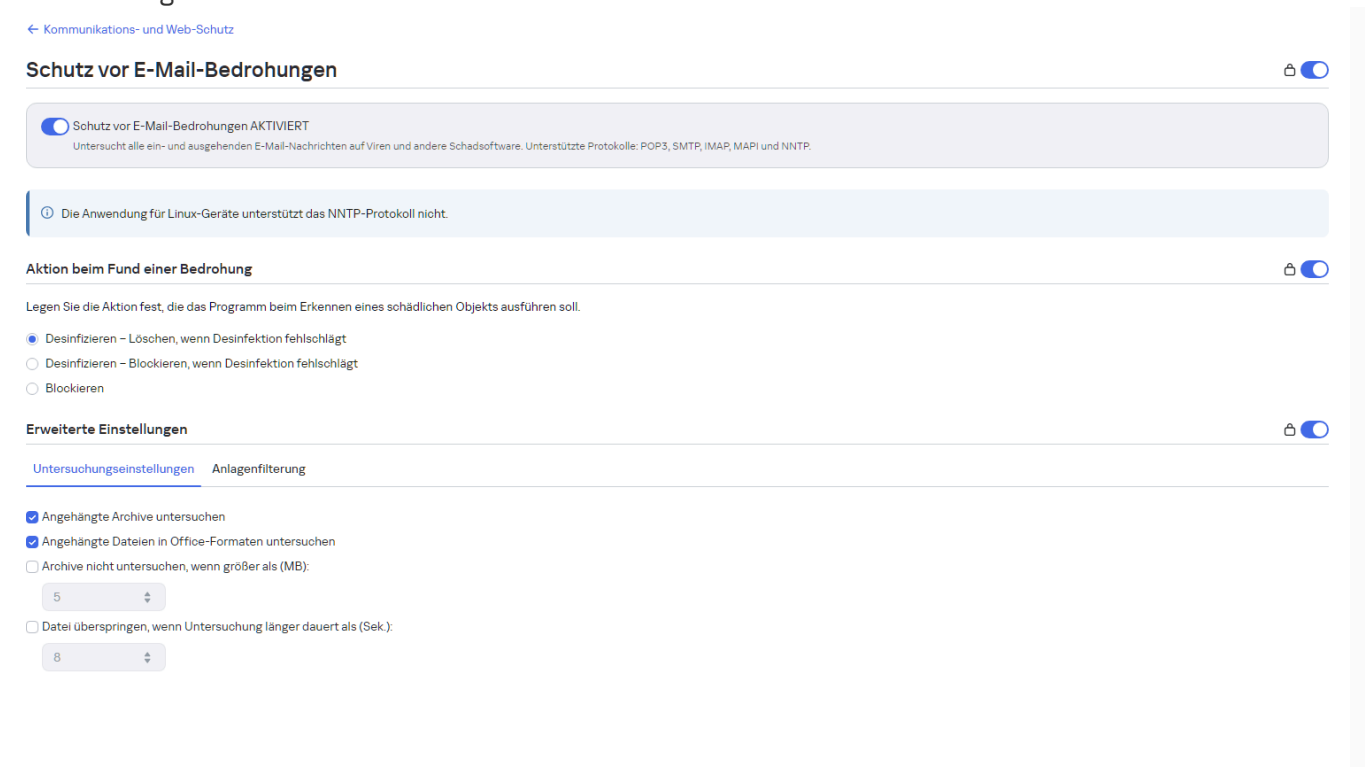
5. Wählen Sie unter **Aktion beim Fund einer Bedrohung** die Aktion aus, die das Programm ausführen soll, wenn eine Bedrohung erkannt wird:

   - **Desinfizieren – Löschen, wenn Desinfektion fehlschlägt**. Wenn ein infiziertes Objekt in einer eingehenden Nachricht erkannt wird, versucht die Anwendung, das Objekt zu desinfizieren. Der Benutzer erhält die Nachricht mit ungefährlichem Anhang. Wenn die Desinfektion fehlschlägt, löscht die Anwendung das infizierte Objekt. Die Anwendung fügt dem Nachrichtenbetreff eine Information über die ausgeführte Aktion hinzu, z. B. *[Nachricht wurde verarbeitet] <Nachrichtenbetreff>*. Wenn ein infiziertes Objekt in einer ausgehenden Nachricht erkannt wird, blockiert die Anwendung den Versand der Nachricht, und der E-Mail-Client zeigt eine Fehlermeldung an.

   - **Desinfizieren – Blockieren, wenn Desinfektion fehlschlägt**. Wenn ein infiziertes Objekt in einer eingehenden Nachricht erkannt wird, versucht die Anwendung, das Objekt zu desinfizieren. Der Benutzer erhält die Nachricht mit ungefährlichem Anhang. Wenn das Objekt nicht desinfiziert werden konnte, fügt die Anwendung dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit ihrem ursprünglichen Anhang. Wenn ein infiziertes Objekt in einer ausgehenden Nachricht erkannt wird, blockiert die Anwendung den Versand der Nachricht, und der E-Mail-Client zeigt eine Fehlermeldung an.

   - **Blockieren**. Wenn ein infiziertes Objekt in einer eingehenden Nachricht erkannt wird, fügt die Anwendung dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit ihrem ursprünglichen Anhang. Wenn ein infiziertes Objekt in einer ausgehenden Nachricht erkannt wird, blockiert die Anwendung den Versand der Nachricht, und der E-Mail-Client zeigt eine Fehlermeldung an.

6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Schutz vor E-Mail-Bedrohungen

So konfigurieren Sie Aktionen beim Erkennen von Bedrohungen über die Befehlszeile

1. Stellen Sie sicher, dass die Komponente „Schutz vor E-Mail-Bedrohungen“ aktiviert ist:

   ```
   kesl-control --get-task-state 35
   ```

   Die Komponente muss den Status **Gestartet** haben.

2. Wenn die Komponente deaktiviert ist, führen Sie den Befehl aus:

   ```
   kesl-control --start-task 35
   ```

3. Wählen Sie eine Aktion aus, die ausgeführt werden soll, wenn in eingehenden Nachrichten eine E-Mail-Bedrohung erkannt wird:

   ```
   kesl-control --set-settings 35 ActionOnThreat=<DisinfectDeleteIfNotPossible|DisinfectBlockIfNotPossible|Block>
   ```

4. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --get-settings 35
   ```

Symbole

Befehlsoptionen

Parameter	Description
`ActionOnThreat`	Aktion beim Erkennen einer Bedrohung: • `DisinfectDeleteIfNotPossible` (Standardeinstellung). Wenn ein infiziertes Objekt in einer eingehenden Nachricht erkannt wird, versucht die Anwendung, das Objekt zu desinfizieren. Der Benutzer erhält die Nachricht mit ungefährlichem Anhang. Wenn die Desinfektion fehlschlägt, löscht die Anwendung das infizierte Objekt. Die Anwendung fügt dem Nachrichtenbetreff eine Information über die ausgeführte Aktion hinzu, z. B. *[Nachricht wurde verarbeitet] <Nachrichtenbetreff>*. Wenn ein infiziertes Objekt in einer ausgehenden Nachricht erkannt wird, blockiert die Anwendung den Versand der Nachricht, und der E-Mail-Client zeigt eine Fehlermeldung an. • `DisinfectBlockIfNotPossible`. Wenn ein infiziertes Objekt in einer eingehenden Nachricht erkannt wird, versucht die Anwendung, das Objekt zu desinfizieren. Der Benutzer erhält die Nachricht mit ungefährlichem Anhang. Wenn das Objekt nicht desinfiziert werden konnte, fügt die Anwendung dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit ihrem ursprünglichen Anhang. Wenn ein infiziertes Objekt in einer ausgehenden Nachricht erkannt wird, blockiert die Anwendung den Versand der Nachricht, und der E-Mail-Client zeigt eine Fehlermeldung an. • `Block`. Wenn ein infiziertes Objekt in einer eingehenden Nachricht erkannt wird, fügt die Anwendung dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit ihrem ursprünglichen Anhang. Wenn ein infiziertes Objekt in einer ausgehenden Nachricht erkannt wird, blockiert die Anwendung den Versand der Nachricht, und der E-Mail-Client zeigt eine Fehlermeldung an.

So optimieren Sie die Untersuchung von E-Mail-Anhängen

Konfigurieren Sie die Untersuchung von E-Mail-Anhängen, um die Komponente Schutz vor E-Mail-Bedrohungen zu optimieren. Dadurch wird die CPU-Auslastung auf dem geschützten Gerät reduziert. Sie können die Untersuchung angehängter Archive einschränken, die maximale Größe der zu untersuchenden Anhänge festlegen und die maximale Dauer der Untersuchung von Objekten festlegen.

So optimieren Sie die Untersuchung von Anhängen in Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Kommunikations- und Web-Schutz → Schutz vor E-Mail-Bedrohungen**.
5. Wählen Sie unter **Erweiterte Einstellungen** die Registerkarte **Untersuchungseinstellungen** aus.
6. Konfigurieren Sie die Untersuchung von Anhängen:

   - **Angehängte Archive untersuchen**. Untersucht Archive der Formate ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE und mehr. Die Anwendung durchsucht Archive nicht nur nach Dateiendung, sondern auch nach Format. Bei der Untersuchung von Archiven entpackt die Anwendung diese rekursiv. Dadurch können Bedrohungen in verschachtelten Archiven (d. h. Archive in Archiven) erkannt werden.
   - **Angehängte Dateien in Office-Formaten untersuchen**. Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte. Die Anwendung untersucht Office-Dateien, die kleiner als 1 MB sind, unabhängig vom Status des Kontrollkästchens.
   - **Archive nicht untersuchen, wenn größer als (MB)**. Wenn das Kontrollkästchen aktiviert ist, schließt die Komponente zum Schutz vor E-Mail-Bedrohungen jene E-Mail-Anhänge, die größer als der angegebene Wert sind, von der Untersuchung aus. Wenn dieses Kontrollkästchen deaktiviert ist, untersucht der Schutz vor E-Mail-Bedrohungen Archive beliebiger Größe, die an E-Mail-Nachrichten angehängt sind.
   - **Datei überspringen, wenn Untersuchung länger dauert als (Sek.)**. Wenn das Kontrollkästchen aktiviert ist, wird die Zeit für die Untersuchung der Archive, die an E-Mail-Nachrichten angehängt sind, auf die eingegebene Dauer beschränkt.
7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So optimieren Sie die Untersuchung von Anhängen über die Befehlszeile

1. Stellen Sie sicher, dass die Komponente „Schutz vor E-Mail-Bedrohungen“ aktiviert ist:

   ```
   kesl-control --get-task-state 35
   ```
2. Die Komponente muss den Status `Started` haben.
3. Wenn die Komponente deaktiviert ist, führen Sie den Befehl aus:

   ```
   kesl-control --start-task 35
   ```

4. Wählen Sie eine Aktion aus, die ausgeführt werden soll, wenn in eingehenden Nachrichten eine E-Mail-Bedrohung erkannt wird:

```
kesl-control --set-settings 35 [ScanFileArchive=<Yes|No>] [UseSizeLimit=<Yes|No>] [SizeLimit=<archive size
(MB)>] [UseTimeLimit=<Yes|No>] [TimeLimit=<scan time (sec)>] [ScanFileOffice=<Yes|No>]
```

5. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 35
```

Symbole

Befehlsoptionen

Parameter	Description
`ScanFileArchive`	Untersucht Archive der Formate ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE und mehr. Die Anwendung durchsucht Archive nicht nur nach Dateiendung, sondern auch nach Format. Bei der Untersuchung von Archiven entpackt die Anwendung diese rekursiv. Dadurch können Bedrohungen in verschachtelten Archiven (d. h. Archive in Archiven) erkannt werden. Standardmäßig untersucht das Programm angehängte Archive.
`UseSizeLimit` `SizeLimit`	Beschränkt die Größe angehängter Archive, die untersucht werden können. Der Schutz vor E-Mail-Bedrohungen überspringt ein angehängtes Archiv bei der Untersuchung, wenn dessen Größe den angegebenen Wert überschreitet. Standardmäßig untersucht das Programm Archive beliebiger Größe.
`UseTimeLimit` `TimeLimit`	Zeitlimit für die Untersuchung angehängter Archive. Standardmäßig ist die Untersuchungszeit für angehängte Archive nicht begrenzt.
`ScanFileOffice`	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte. Die Anwendung untersucht Office-Dateien, die kleiner als 1 MB sind, unabhängig vom Status des Kontrollkästchens. Standardmäßig untersucht das Programm angehängte Dateien im Office-Format.

Wozu ein Filter für E-Mail-Anhänge dient

Die Anlagenfilterung funktioniert nicht für ausgehende E-Mail-Nachrichten.

Schädliche Programme können sich in Form von den Anlagen für E-Mail-Nachrichten verbreiten. Sie können eine Filterung nach dem Typ der Nachrichtenanhänge einrichten, damit Dateien der festgelegten Typen automatisch umbenannt oder gelöscht werden. Durch das Umbenennen bestimmter Typen kann Kaspersky Endpoint Security Ihren Computer vor dem automatischen Start von schädlichen Programmen schützen.

Sie können beispielsweise die Filterung von Anhängen für HTML-Dateien konfigurieren. Eine HTML-Datei kann schädliche Skripts enthalten. Wenn das Programm eine solche Datei umbenennt, kann der Benutzer die HTML-Seite nicht per Doppelklick in einer E-Mail-Nachricht öffnen. Um die HTML-Datei zu öffnen, muss der Benutzer die Datei herunterladen und umbenennen. Dadurch hat der Benutzer Zeit, die empfangene Nachricht zu analysieren und die Ausführung des schädlichen Skripts zu verhindern.

Standardmäßig benennt das Programm Dateien mit den Erweiterungen CMD, COM, EXE, JS, JSE, MSI, SCR, VBE, VBS, SH um. Das Programm ersetzt bei den angegebenen Dateitypen das letzte Zeichen der Erweiterung durch einen Unterstrich (z. B. attachment.doc_).

So konfigurieren Sie den Filter für E-Mail-Anhänge in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Kommunikations- und Web-Schutz** → **Schutz vor E-Mail-Bedrohungen**.
5. Wählen Sie unter **Erweiterte Einstellungen** die Registerkarte **Anlagenfilterung** aus.
6. Wählen Sie die Aktion aus, die das Programm auf den E-Mail-Anhang anwenden soll:

   - **Anlagen nicht verändern**. Wenn diese Option ausgewählt ist, filtert der Schutz vor E-Mail-Bedrohungen keine an E-Mail-Nachrichten angehängten Dateien.
   - **Anlagen der ausgewählten Typen umbenennen**. Wenn diese Option ausgewählt ist, ersetzt der Schutz vor E-Mail-Bedrohungen das letzte Zeichen der Dateierweiterung von angehängten Dateien der angegebenen Typen durch einen Unterstrich (z. B. attachment.doc_). Wenn ein Benutzer die Datei öffnen möchte, muss er sie daher zunächst umbenennen.
   - **Anlagen der ausgewählten Typen löschen**. Wenn diese Option ausgewählt ist, entfernt der Schutz vor E-Mail-Bedrohungen Anhänge mit den angegebenen Dateitypen aus E-Mail-Nachrichten.
7. Wenn Sie im vorherigen Schritt die Option **Anlagen der ausgewählten Typen umbenennen** oder **Anlagen der ausgewählten Typen löschen** ausgewählt haben, aktivieren Sie die Kontrollkästchen für die entsprechenden Dateitypen.
8. Wenn der benötigte Dateityp nicht aufgeführt ist, fügen Sie einen neuen Anhangstyp hinzu:

   a. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Dadurch wird das Formular zum Hinzufügen eines neuen Anhangstyps geöffnet.

   b. Geben Sie im Feld **Anlagentypen** die Erweiterungsmasken im Format `*.<extension>` (z. B. `*.doc`) an.

   Wenn Sie mehrere Dateitypen angeben möchten, geben Sie jeden Dateityp in einer neuen Zeile ein.
9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie den Filter für E-Mail-Anhänge über die Befehlszeile

1. Stellen Sie sicher, dass die Komponente „Schutz vor E-Mail-Bedrohungen" aktiviert ist:

   ```
   kesl-control --get-task-state 35
   ```
2. Die Komponente muss den Status `Started` haben.
3. Wenn die Komponente deaktiviert ist, führen Sie den Befehl aus:

   ```
   kesl-control --start-task 35
   ```

4. Wählen Sie die Aktion aus, die das Programm auf den E-Mail-Anhang anwenden soll:

```
kesl-control --set-settings 35 ExtensionFilter=<Disable|Rename|Delete>
ExtensionMasks.item_#.UseExtensionMask=Yes\
[ExtensionMasks=*.<extention>]
```

5. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 35
```

Symbole

Befehlsoptionen

Parameter	Description
`ExtensionFilter`	Die Aktion, die das Programm auf den E-Mail-Anhang anwenden soll: `Disable`. Wenn diese Option ausgewählt ist, filtert der Schutz vor E-Mail-Bedrohungen keine an E-Mail-Nachrichten angehängten Dateien. `Rename` (Standardeinstellung). Wenn diese Option ausgewählt ist, ersetzt der Schutz vor E-Mail-Bedrohungen das letzte Zeichen der Dateierweiterung von angehängten Dateien der angegebenen Typen durch einen Unterstrich (z. B. attachment.doc_). Wenn ein Benutzer die Datei öffnen möchte, muss er sie daher zunächst umbenennen. `Delete`. Wenn diese Option ausgewählt ist, entfernt der Schutz vor E-Mail-Bedrohungen Anhänge mit den angegebenen Dateitypen aus E-Mail-Nachrichten.
`UseExtensionMask=Yes`	Hinzufügen eines Dateityps zum Filter für E-Mail-Anhänge. Sie können einen Dateityp vorübergehend vom Filter für E-Mail-Anhänge ausschließen, anstatt ihn zu entfernen. Legen Sie dazu `ExtensionMasks.item_#.UseExtensionMask=No` fest
`ExtensionMasks=*.<extention>`	Erweiterung des Anhangstyps, den Sie umbenennen oder aus E-Mail-Nachrichten entfernen möchten.

Schutz vor Web-Bedrohungen

Die Komponente „Schutz vor Web-Bedrohungen“ verhindert den Download schädlicher Dateien aus dem Internet und blockiert außerdem Verbindungen zu schädlichen Websites und Phishing-Websites. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes "Kaspersky Security Network" und der heuristischen Analyse.

Funktionsweise des Schutzes vor Web-Bedrohungen

Bei der Installation von Kaspersky Endpoint Security fügt das Programm ein selbstsigniertes Zertifikat hinzu: *Persönliches Root-Zertifikat von Kaspersky Anti-Virus*. Die App legt dieses Zertifikat im lokalen Speicher für vertrauenswürdige Zertifikate (`/etc/ssl/certs`) und im Zertifikatspeicher der Webbrowser ab. Bei jedem Programmstart prüft es, ob das Zertifikat vorhanden ist. Wenn das Zertifikat gelöscht wurde, stellt das Programm es automatisch wieder her.

1. **Abfangen einer ausgehenden Verbindung**

   Eine Drittanbieter-App (z. B. ein Browser) initiiert eine Verbindung mit einem Server. Kaspersky Endpoint Security ersetzt das Serverzertifikat durch ein eigenes Zertifikat, das mit dem Persönlichen Stammzertifikat von Kaspersky Anti-Virus signiert ist. Anschließend fängt die App den Verschlüsselungsschlüssel ab und entschlüsselt die Kommunikationssitzung. Kaspersky Endpoint Security führt diesen Vorgang ohne Benachrichtigung des Benutzers aus, da sich das Persönliche Stammzertifikat von Kaspersky Anti-Virus im Speicher für vertrauenswürdige Zertifikate befindet.

2. **Netzwerkverkehr untersuchen**

Der Schutz vor Web-Bedrohungen untersucht den Datenverkehr mithilfe folgender Technologien:

- Antiviren-Datenbanken.
- Cloud-Dienste von Kaspersky Security Network.
- Die Technologie der heuristischen Analyse ermöglicht die Erkennung von Bedrohungen, die noch nicht in den Kaspersky-Datenbanken erfasst sind.

3. **Abschluss der Untersuchung**

   Wenn eine Website als schädliche oder Phishing-Website eingestuft wird, führt Kaspersky Endpoint Security die Aktion aus, die in den Einstellungen der Komponente Schutz vor Web-Bedrohungen festgelegt ist: Die Verbindung wird entweder blockiert oder es wird eine Warnung angezeigt.

Einstellungen für den Schutz vor Web-Bedrohungen

1. **Regeln der Firewall des Betriebssystems konfigurieren**

   Wenn das System über eigene Netzwerkregeln oder firewalld-Regeln mit Drop-Richtlinien verfügt, müssen Sie eine Regel hinzufügen, die eingehende Verbindungen vom lokalen Gerät (Loopback) erlaubt, damit die App ordnungsgemäß funktioniert:

   Beispielbefehl für iptables:

   ```
   iptables -A INPUT -i lo -j ACCEPT
   ```

2. **Modus zum Abfangen des Netzwerkdatenverkehrs auswählen**

   Beim Empfang von Netzwerkpaketen extrahiert der Schutz vor Web-Bedrohungen Daten zur Untersuchung auf Bedrohungen. Die folgenden Modi zum Abfangen des Netzwerkdatenverkehrs können verwendet werden:

   - eBPF
   - iptables (Standard)

   Die Wahl des Modus zum Abfangen des Netzwerkdatenverkehrs hängt von der Infrastruktur der Organisation ab. In einem geschlossenen Perimeter empfehlen wir die Verwendung von eBPF. Verwenden Sie in anderen Szenarien iptables.

   > Wir empfehlen, Geräte je nach Modus zum Abfangen des Netzwerkdatenverkehrs in verschiedene Administrationsgruppen einzuteilen.

3. **Richtlinie für die Zertifikatsvalidierung konfigurieren**

   Standardmäßig entschlüsselt und untersucht Schutz vor Web-Bedrohungen den Netzwerkverkehr, der über verschlüsselte Verbindungen übertragen wird. Darüber hinaus kann die Komponente das Internet verwenden, um fehlende Ketten, die zur Überprüfung des Zertifikats erforderlich sind, zu überprüfen und herunterzuladen. Wenn das Gerät keinen direkten Internetzugang hat, müssen Sie eine lokale Methode zur Zertifikatsvalidierung auswählen (ohne Internetnutzung) oder einen Proxyserver für den Internetzugang verwenden.

Die Richtlinie für die Zertifikatsvalidierung umfasst außerdem die folgenden Einstellungen:

- Zugriff auf Websites mit einem nicht vertrauenswürdigen Zertifikat
- Zugriff auf Websites mit einem Fehler bei der Zertifikatsvalidierung

Standardmäßig erlaubt Kaspersky Endpoint Security den Zugriff auf Websites mit einem nicht vertrauenswürdigen Zertifikat und fügt die Domäne, bei der ein Fehler bei der Zertifikatsvalidierung auftritt, zu den Ausnahmen hinzu. Fehler bei der Zertifikatsvalidierung können beispielsweise bei der Verwendung von Banking-Anwendungen oder Cloud-Speichern auftreten. Die Domänen, zu denen diese Dienste gehören, können das persönliche Stammzertifikat von Kaspersky Anti-Virus ablehnen. Sie können Ihre eigene Richtlinie für die Zertifikatsvalidierung konfigurieren.

4. **Vertrauenswürdige Zertifikate hinzufügen**

   Wenn Ihre Organisation private Zertifizierungsstellen verwendet, um Zertifikate für interne Server auszustellen, kann Kaspersky Endpoint Security den Zugriff auf Webressourcen aufgrund von Fehlern bei der Zertifikatsvalidierung blockieren. Fügen Sie diese Zertifikate zur Liste der vertrauenswürdigen Zertifikate hinzu, um Webressourcen von der Untersuchung verschlüsselter Verbindungen auszuschließen.

5. **Wählen Sie in den Einstellungen für den Schutz vor Web-Bedrohungen die Aktion „Informieren“ aus**

   Standardmäßig ist der Schutz vor Web-Bedrohungen deaktiviert. Wir empfehlen, den Schutz vor Web-Bedrohungen zu aktivieren, als Aktion beim Erkennen einer Bedrohung die Option **Informieren** auszuwählen und den Zugriff auf alle Unternehmensressourcen zu überprüfen. Kaspersky Endpoint Security erlaubt den Zugriff auf alle Websites und protokolliert Informationen über erkannte Bedrohungen.

6. **Statistiken zu Websites erfassen, die der Schutz vor Web-Bedrohungen als unsicher einstuft**

   Sie können mithilfe von Berichten Statistiken zu Websites abrufen, die der Schutz vor Web-Bedrohungen als unsicher einstuft.

7. **Vertrauenswürdige Webadressen hinzufügen**

   Nachdem Sie die Berichte zum Schutz vor Web-Bedrohungen überprüft haben, müssen Sie der Liste der vertrauenswürdigen Webadressen Webadressen hinzufügen, denen Sie vertrauen. Wenn die Liste der vertrauenswürdigen Webadressen nicht ausreicht, um den Konflikt zwischen Kaspersky Endpoint Security und Drittanbieter-Programmen zu beheben, können Sie die spezielle Kette von Erlaubnisregeln kesl_bypass verwenden. Die *kesl_bypass-Kette* ist eine spezielle Regelliste, die Kaspersky Endpoint Security in der mangle-Tabelle der Firewall des Betriebssystems (iptables/ip6tables) erstellt.

8. **Wählen Sie in den Einstellungen für den Schutz vor Web-Bedrohungen die Aktion „Blockieren“ aus**

   Blockieren infizierter Objekte im Web-Datenverkehr aktivieren.

Besonderheiten und Einschränkungen

- Das Programm untersucht den eingehenden Datenverkehr an TCP-Ports und verwendet Port 9879 auf localhost, um Verbindungen abzufangen. Wenn Port 9879 bereits belegt ist, wählt das Programm automatisch einen verfügbaren Port aus, um Verbindungen abzufangen.
- Beim Aktivieren oder Deaktivieren des Programms sowie beim Aktivieren oder Deaktivieren der Komponenten „Schutz vor Web-Bedrohungen“ und „Schutz vor Netzwerkbedrohungen“ werden Verbindungen an abgefangenen Ports beendet.
- Kaspersky Endpoint Security untersucht den HTTP- und HTTPS-Datenverkehr. Kaspersky Endpoint Security untersucht URL- und IP-Adressen.

- Die App unterstützt die folgenden ausführbaren Dateien von Browsern, auch im Snap-Format:
  - chrome
  - chromium
  - chromium-browser
  - firefox
  - firefox-esr
  - google-chrome
  - opera
  - yandex-browser
- Wenn ein Benutzer versucht, eine schädliche Website zu besuchen, führt die App folgende Aktionen aus:
  - **HTTP**. Die App blockiert den Zugriff und zeigt eine Warnung an.
  - **HTTPS**. Die App blockiert den Zugriff; der Browser zeigt eine Fehlerseite an.
- Das Entfernen von Anwendungszertifikaten kann zu einer fehlerhaften Ausführung der Komponente „Schutz vor Web-Bedrohungen“ führen.

Nützliche Artikel

Was tun, wenn die Warnung „Besuch einer Domain mit nicht vertrauenswürdigem Zertifikat“ angezeigt wird

Aktion beim Fund einer Web-Bedrohung auswählen

Wenn eine Web-Bedrohung gefunden wird, kann Kaspersky Endpoint Security den Zugriff auf gefährliche Objekte blockieren oder nur über den Fund eines gefährlichen Objekts informieren.

Aktionen beim Fund einer Web-Bedrohung in der Web Console konfigurieren

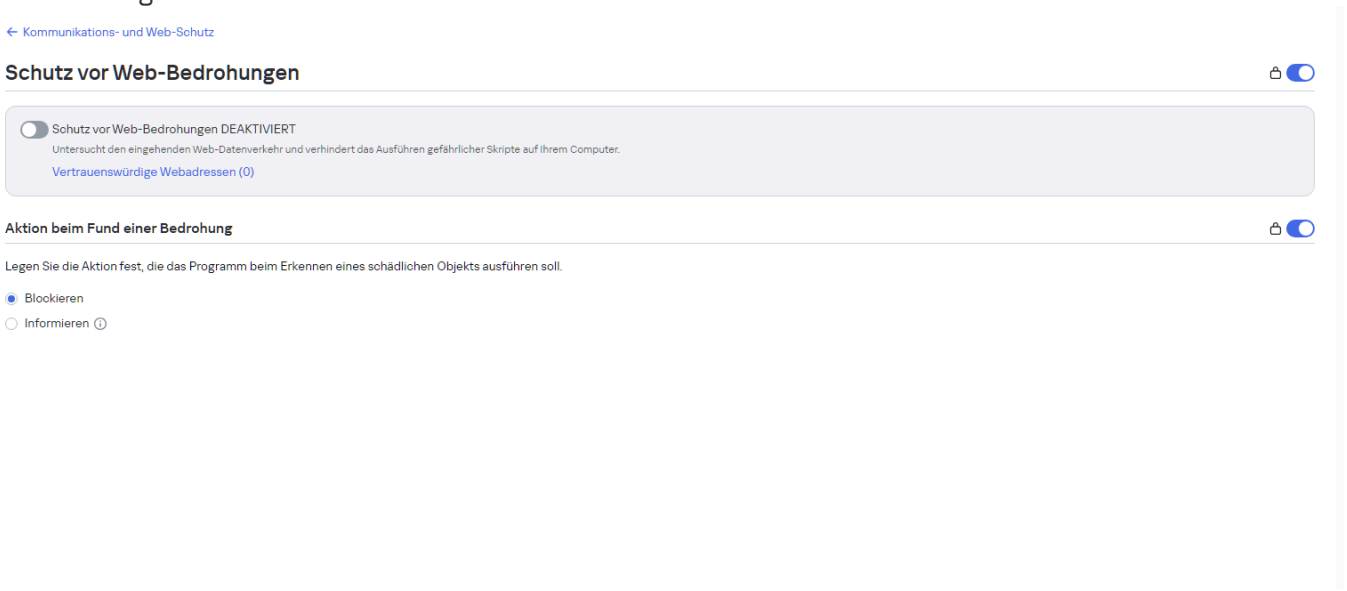
1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Kommunikations- und Web-Schutz** → **Schutz vor Web-Bedrohungen**.

5. Wählen Sie unter **Aktion beim Fund einer Bedrohung** die Aktion aus, die das Programm ausführen soll, wenn eine Bedrohung erkannt wird:

   - **Blockieren**. Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so blockiert die Komponente „Schutz vor Web-Bedrohungen“ den Zugriff auf das Objekt und zeigt im Browser eine Benachrichtigung an.

   - **Informieren**. Kaspersky Endpoint Security informiert den Benutzer über den Fund eines infizierten Objekts im Web-Datenverkehr. Der Schutz vor Web-Bedrohungen ermöglicht das Herunterladen dieses Objekts auf das Gerät. Dabei protokolliert die Anwendung die Informationen über das infizierte Objekt und fügt es zur Liste der aktiven Bedrohungen hinzu.

6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Schutz vor Web-Bedrohungen

So konfigurieren Sie Aktionen beim Erkennen von Bedrohungen über die Befehlszeile

1. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control --set-settings 14 ActionOnDetect=<Block|Notify>
   ```

2. Wählen Sie die Datenbanken aus, die für die Untersuchung von Links verwendet werden sollen:

   ```
   kesl-control --set-settings 14 CheckMalicious=<Yes|No> CheckAdware=<Yes|No> CheckOther=<Yes|No>
   ```

3. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --get-settings 14
   ```

Symbole

Parameter	Description
`ActionOnDetect`	Aktion beim Erkennen einer Bedrohung: • `Block` (Standardeinstellung). Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so blockiert die Komponente „Schutz vor Web-Bedrohungen“ den Zugriff auf das Objekt und zeigt im Browser eine Benachrichtigung an. • `Notify`. Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so erlaubt Kaspersky Endpoint Security den Download dieses Objekts auf den Computer und fügt Informationen über das infizierte Objekt zur Liste der aktiven Bedrohungen hinzu.
`CheckMalicious`	Es wird überprüft, ob Links in der Datenbank für bösartige Webadressen vorhanden sind. Das ermöglicht den Schutz vor Websites, die auf der Deny-Liste stehen. Die Datenbank für schädliche Webadressen wird von den Kaspersky-Fachleuten angelegt, gehört zum Lieferumfang des Programms und wird beim Datenbank-Update von Kaspersky Endpoint Security aktualisiert. Die Untersuchung ist standardmäßig aktiviert (`Yes`).
`CheckAdware`	Untersuchung von Links anhand der Datenbank für Werbe-Webadressen. Die Untersuchung ist standardmäßig deaktiviert (`No`).
`CheckOther`	Untersuchung von Links anhand der Datenbank für Webadressen, die legitime Anwendungen enthalten, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können. Die Untersuchung ist standardmäßig deaktiviert (`No`).

Was ist Anti-Phishing

Der „Schutz vor Web-Bedrohungen“ untersucht Links, um festzustellen, ob sie zu Phishing-Webadressen gehören. Dadurch können *Phishing-Angriffe* verhindert werden. Ein häufiges Beispiel für Phishing-Angriffe ist eine E-Mail-Nachricht, die scheinbar von Ihrer Bank stammt und einen Link zur offiziellen Website der Bank enthält. Wenn Sie dem Link folgen, gelangen Sie auf eine Website, die eine exakte Kopie der Bankseite darstellt und für die im Browser sogar deren Webadresse angezeigt wird, obwohl Sie sich in Wirklichkeit auf einer fiktiven Website befinden. Alle Aktionen, die Sie auf dieser Website ausführen, werden verfolgt und können zum Diebstahl Ihres Geldes missbraucht werden.

Phishing-Links können sich nicht nur in E-Mail-Nachrichten befinden, sondern beispielsweise auch in Messengern. Darum überwacht die Komponente „Schutz vor Web-Bedrohungen“ alle Versuche zum Öffnen einer Phishing-Website auf der Ebene des Web-Datenverkehrs und blockiert den Zugriff auf solche Websites. Listen mit Phishing-Webadressen gehören zum Lieferumfang von Kaspersky Endpoint Security.

Sie können die Anti-Phishing-Funktionalität nur über die Befehlszeile konfigurieren. Anti-Phishing kann nicht in der Web Console konfiguriert werden. „Anti-Phishing“ ist standardmäßig mit der heuristischen Analyse aktiviert.

So aktivieren Sie Anti-Phishing über die Befehlszeile

1. Stellen Sie sicher, dass die Komponente Schutz vor Web-Bedrohungen aktiviert ist:

   ```
   kesl-control --get-task-state 14
   ```

   Die Komponente muss den Status **Gestartet** haben.

2. Wenn die Komponente deaktiviert ist, führen Sie den Befehl aus:

   ```
   kesl-control --start-task 14
   ```

3. Aktivieren Sie Anti-Phishing:

```
kesl-control --set-settings 14 CheckPhishing=Yes
```

4. Konfigurieren Sie die heuristische Analyse für die Untersuchung von Webseiten auf Phishing-Links:

```
kesl-control --set-settings 14 UseHeuristicForPhishing=<Yes|No>
```

Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.

5. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 14
```

Schutz vor Netzwerkbedrohungen

Die Komponente *Schutz vor Netzwerkbedrohungen* (auch Intrusion Detection System oder IDS genannt) überwacht den eingehenden Netzwerkverkehr auf Aktivitäten, die für Netzwerkangriffe charakteristisch sind. Wenn das Programm einen Netzwerkangriff auf den Benutzercomputer erkennt, sperrt es die Netzwerkverbindung mit dem angreifenden Computer. Beschreibungen der derzeit bekannten Arten von Netzwerkangriffen und entsprechende Abwehrmethoden sind in den Programm-Datenbanken enthalten. Die Liste der Netzwerkangriffe, die von der Komponente "Schutz vor Netzwerkbedrohungen" erkannt werden, wird beim Update der Datenbanken und Programm-Module aktualisiert.

Funktionsweise des Schutzes vor Netzwerkbedrohungen

1. **Das Programm analysiert eingehende Pakete**

   Zur Untersuchung des eingehenden Datenverkehrs erhält die Komponente „Schutz vor Netzwerkbedrohungen“ Portnummern aus den Datenbanken des Programms und akzeptiert Verbindungen über alle diese Ports. Während der Netzwerkuntersuchung im iptables-Modus zum Abfangen des Datenverkehrs kann es so aussehen, als wäre auf dem Gerät ein Port geöffnet, auch wenn keine Anwendung im System diesen Port überwacht. Wir empfehlen, nicht verwendete Ports mithilfe einer Firewall zu schließen.

2. **Das Programm untersucht den eingehenden Datenverkehr**

   Der Schutz vor Netzwerkbedrohungen untersucht den eingehenden Datenverkehr mithilfe der folgenden Technologien:

   - Antiviren-Datenbanken.
   - Cloud-Dienste von Kaspersky Security Network.
   - Die Technologie der heuristischen Analyse ermöglicht die Erkennung von Bedrohungen, die noch nicht in den Kaspersky-Datenbanken erfasst sind.

3 Abschluss der Untersuchung

Wenn eine Netzwerkbedrohung erkannt wird, blockiert das Programm für einen festgelegten Zeitraum alle Netzwerkverbindungen des angreifenden Geräts.

Einstellungen für den Schutz vor Netzwerkbedrohungen

1 Regeln der Firewall des Betriebssystems konfigurieren

Um die Kompatibilität von REDIRECT-Regeln (z. B. Umleitung von Port 443 auf Port 8443) mit den Regeln zum Abfangen des Datenverkehrs durch den Schutz vor Netzwerkbedrohungen zu gewährleisten, müssen Sie die REDIRECT-Regeln löschen und Regeln zum Abfangen des Datenverkehrs hinzufügen.

Beispiel für einen Befehl zum Löschen von REDIRECT-Regeln:

```
iptables -t nat -D PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
```

Beispiel für Befehle zum Hinzufügen von Regeln zum Abfangen des Datenverkehrs:

```
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -m mark ! --mark 0x400/0x400 -j REDIRECT --to-ports 8443
```

```
iptables -t nat -A OUTPUT -p tcp --dport 443 -m mark --mark 0x400/0x400 -m addrtype ! --src-type LOCAL -j DNAT -
-to-destination :8443
```

2 Liste der zu kontrollierenden Netzwerkports erstellen

Standardmäßig überwacht die Anwendung bekannte und registrierte Ports, beispielsweise Port 443 für HTTPS-Verbindungen und Port 143 für das E-Mail-Protokoll IMAP. Die Standardeinstellungen bieten das empfohlene Schutzniveau und eine optimale Ressourcennutzung. Bei Bedarf können Sie die Liste der kontrollierten Ports ändern oder die Kontrolle für alle Ports aktivieren.

3 Modus zum Abfangen des Datenverkehrs auswählen

Beim Empfang von Netzwerkpaketen extrahiert der Schutz vor Netzwerkbedrohungen Daten, um sie auf Bedrohungen zu untersuchen. Für das Abfangen des eingehenden Datenverkehrs können die folgenden Modi verwendet werden:

- eBPF
- iptables (Standard)

Die Wahl des Modus zum Abfangen des Datenverkehrs hängt von der Infrastruktur der Organisation ab. In einem geschlossenen Perimeter empfehlen wir die Verwendung von eBPF. Verwenden Sie in anderen Szenarien iptables.

> Wir empfehlen, Geräte je nach Modus zum Abfangen des Datenverkehrs in verschiedene Administrationsgruppen zu gruppieren.

4. **Schutz vor Web-Bedrohungen im Informationsmodus aktivieren**

   Standardmäßig ist der Schutz vor Netzwerkbedrohungen deaktiviert. Bevor Sie den Schutz vor Netzwerkbedrohungen im Modus „Blockieren“ aktivieren, empfehlen wir, die Komponente im Modus „Informieren“ zu aktivieren. Dadurch kann Kaspersky Endpoint Security verdächtige Netzwerkaktivitäten erkennen und Informationen über erkannte Netzwerkangriffe protokollieren, ohne Netzwerkverbindungen zu unterbrechen. Überprüfen Sie den Zugriff von Unternehmensanwendungen von Drittanbietern auf Netzwerkressourcen. Stellen Sie sicher, dass die Kontrolle von Netzwerkports diese Anwendungen nicht verlangsamt.

5. **Statistiken für IP-Adressen erfassen, bei denen der Schutz vor Netzwerkbedrohungen verdächtige Netzwerkaktivitäten feststellt**

   Sie können Berichte anzeigen, um Statistiken für IP-Adressen abzurufen, die der Schutz vor Netzwerkbedrohungen als unsicher einstuft. Die Anwendung generiert *Netzwerkangriff erkannt*-Ereignisse.

6. **Vertrauenswürdige IP-Adressen hinzufügen**

   Nachdem Sie die Berichte zum Schutz vor Netzwerkbedrohungen überprüft haben, müssen Sie die IP-Adressen der Geräte, deren Netzwerkverbindungen Sie vertrauen, zur Liste der vertrauenswürdigen Geräte hinzufügen. Sie können die Adresse eines einzelnen Geräts oder Subnetzes zur Liste der Ausnahmen hinzufügen. Der Schutz vor Netzwerkbedrohungen fängt Pakete von einem solchen Gerät nicht ab und untersucht sie nicht.

7. **Schutz vor Netzwerkbedrohungen im Modus „Blockieren“ aktivieren**

   Nachdem Sie die IP-Adressen vertrauenswürdiger Geräte zur Liste der Ausnahmen hinzugefügt haben, aktivieren Sie die Komponente im Modus „Blockieren“. Die Netzwerkaktivität von nicht vertrauenswürdigen Geräten wird blockiert, und entsprechende Informationen werden in Berichten angezeigt.

Besonderheiten und Einschränkungen

- Die App untersucht den eingehenden Datenverkehr an TCP-Ports. Die App verwendet auf localhost den festen Port 9789, um Verbindungen abzufangen.
- Beim Aktivieren oder Deaktivieren des Programms sowie beim Aktivieren oder Deaktivieren der Komponenten „Schutz vor Web-Bedrohungen“ und „Schutz vor Netzwerkbedrohungen“ werden Verbindungen an abgefangenen Ports beendet.
- Der Schutz vor Netzwerkbedrohungen funktioniert nicht auf Computern mit CentOS 5.2 oder 5.4, da diese TProxy nicht unterstützen.

So wählen Sie eine Aktion bei der Erkennung von Netzwerkbedrohungen aus

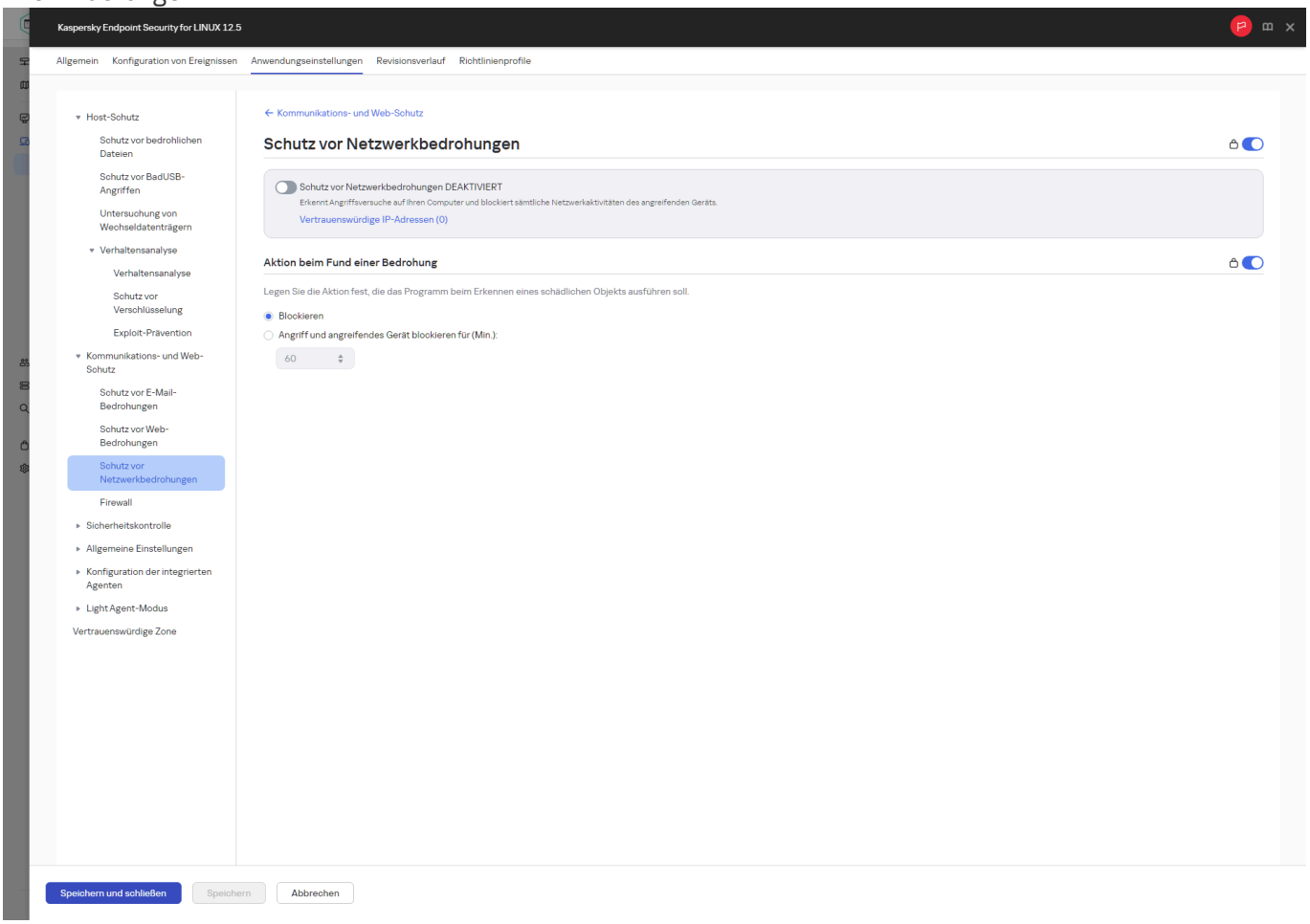
Wenn ein versuchter Netzwerkangriff auf ein geschütztes Gerät erkannt wird, blockiert die App die Netzwerkaktivität des angreifenden Geräts und erstellt ein Ereignis *Netzwerkangriff erkannt*.

Um den Netzwerkverkehr zu blockieren, erstellt Kaspersky Endpoint Security eine dynamische Firewall-Regel. Die Firewall blockiert vorübergehend den Netzwerkverkehr für das angreifende Gerät. Die App fügt das kompromittierte Gerät außerdem zur Liste der blockierten Geräte hinzu. Blockierten Geräten wird der Zugriff auf freigegebene Netzwerkverzeichnisse verweigert.

So konfigurieren Sie Aktionen bei der Erkennung von Netzwerkangriffen in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Kommunikations- und Web-Schutz** → **Schutz vor Netzwerkbedrohungen**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **Schutz vor Netzwerkbedrohungen AKTIVIERT** befindet.
6. Aktivieren Sie das Kontrollkästchen **Schutz vor Netzwerkbedrohungen für Linux-Geräte aktivieren**.
7. Wählen Sie unter **Aktion beim Fund einer Bedrohung** die Aktion aus, die die App bei Erkennung einer Bedrohung ausführen soll: **Blockieren** oder **Angriff und angreifendes Gerät blockieren für (Min.)**.
8. Wenn **Angriff und angreifendes Gerät blockieren für (Min.)** ausgewählt ist, legen Sie die Sperrdauer für das kompromittierte Gerät in Minuten fest. Standardmäßig wird das Gerät für 60 Minuten blockiert. Mögliche Werte: 1 bis 999.
9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Schutz vor Netzwerkbedrohungen

So konfigurieren Sie Aktionen bei der Erkennung von Netzwerkangriffen über die Befehlszeile

1. Stellen Sie sicher, dass die Komponente „Schutz vor Netzwerkbedrohungen“ aktiviert ist:

   ```
   kesl-control --get-task-state 17
   ```

   Die Komponente muss den Status **Gestartet** haben.

2. Wenn die Komponente deaktiviert ist, führen Sie den Befehl aus:

   ```
   kesl-control --start-task 17
   ```

3. Wählen Sie eine Aktion bei der Erkennung von Netzwerkbedrohungen aus:

   ```
   kesl-control --set-settings 17 ActionOnDetect=<Block|Notify>
   ```

4. Konfigurieren Sie die Sperrung des kompromittierten Geräts:

   ```
   kesl-control --set-settings 17 BlockAttackingHosts=<Yes|No>
   ```

5. Wählen Sie die Sperrdauer für die Aktion `BlockAttackingHosts=Yes` aus:

   ```
   kesl-control --set-settings 17 BlockDurationMinutes=<Blocking period>
   ```

6. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --get-settings 17
   ```

Symbole

Befehlsoptionen

Parameter	Description
`ActionOnDetect`	Aktion bei der Erkennung von Netzwerkbedrohungen: • `Block` (Standard) blockiert den Netzwerkverkehr des kompromittierten Geräts und erstellt ein Ereignis *Netzwerkangriff erkannt*. • `Notify` erstellt ein *Netzwerkangriff erkannt*-Ereignis, ohne den Netzwerkverkehr zu blockieren.
`BlockAttackingHosts`	Netzwerkaktivität des angreifenden Geräts blockieren. Die Gerätesperrung ist standardmäßig aktiviert.
`BlockDurationMinutes`	Konfigurieren Sie die Sperrdauer für das Remote-Gerät, das an schädlichen Aktivitäten oder schädlicher Datenverschlüsselung beteiligt ist.

Blockierte Geräte verwalten

Beim Schutz eines Geräts vor Netzwerkbedrohungen und bösartiger Remote-Verschlüsselung kann Kaspersky Endpoint Security Remote-Geräte blockieren, deren Aktionen als bösartig eingestuft werden. Geräte werden durch die Komponenten Schutz vor Verschlüsselung und Schutz vor Netzwerkbedrohungen vor Bedrohungen dieser Typen geschützt. Kaspersky Endpoint Security blockiert den Netzwerkverkehr für eine bestimmte Dauer. Wenn die Blockierungsdauer abläuft, lässt Kaspersky Endpoint Security den Netzwerkverkehr wieder zu. Standardmäßig blockiert das Programm den Netzwerkverkehr eines angreifenden Geräts für 60 Minuten. Wenn die Blockierungsdauer abläuft, entfernt das Programm dieses Gerät aus der Liste der blockierten Geräte.

Wenn Kaspersky Endpoint Security ein vertrauenswürdiges Gerät blockiert hat, müssen Sie die IP-Adresse dieses Geräts zur Liste der Ausnahmen hinzufügen.

Liste der blockierten Geräte anzeigen

```
kesl-control -H --get-blocked-hosts
```

Als Ergebnis der Ausführung des Befehls gibt die App die Liste der blockierten Geräte in der Konsole aus.

Liste der blockierten Geräte

```
Blocked devices: 1
Host                : 10.69.119.234
Block date          : 2026-04-29 15:44
Will be unblocked   : 2026-04-29 16:44
Task name           : Network_Threat_Protection
```

Blockierung eines Geräts aufheben

```
kesl-control -H --allow-hosts <address>
```

Dabei steht `<address>` für eine oder mehrere IP-Adressen von Geräten oder Subnetzen (IPv4/IPv6, einschließlich Adressen in Kurzform). Sie können mehrere, durch Leerzeichen getrennte IP-Adressen von Geräten oder Subnetzen angeben.

Firewall-Verwaltung

Die Firewall des Betriebssystems kontrolliert die gesamte Netzwerkaktivität des Geräts, sowohl im Internet als auch im lokalen Netzwerk. Die Firewall schützt die Daten auf dem Gerät vor unbefugtem Zugriff und blockiert die meisten Bedrohungen, z. B. aus dem Netzwerk kommende Angriffe auf das Gerät. Mit der Firewall können alle Netzwerkverbindungen auf dem Gerät des Benutzers erkannt und eine Liste ihrer IP-Adressen abgerufen werden.

Das Programm verwaltet die Firewall des Betriebssystems mithilfe der Komponente Firewall-Verwaltung. Die Komponente fügt der Firewall des Betriebssystems Regeln für Netzwerkpakete hinzu, um die Netzwerkaktivität von Geräten zu überwachen. Mithilfe von Netzwerkpaketregeln können Sie die gewünschte Ebene des Geräteschutzes von der Blockierung des Internetzugangs für alle Anwendungen bis zur Erlaubnis von unbegrenztem Zugang festlegen.

Standardmäßig ist die Komponente "Firewall-Verwaltung" deaktiviert.

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.

Wenn die Firewall-Verwaltung aktiviert ist, überprüft Kaspersky Endpoint Security die Firewall des Betriebssystems alle 60 Sekunden. Wenn die Überprüfung ergibt, dass ein Drittanbieter-Programm oder -Dienstprogramm eine Regel für Netzwerkpakete hinzugefügt oder entfernt hat, stellt Kaspersky Endpoint Security den mit dem Programm erstellten Satz von Firewall-Regeln wieder her.

Kaspersky Endpoint Security überprüft weiterhin die Firewall des Betriebssystems, selbst wenn die Firewall-Verwaltung deaktiviert ist. Das ermöglicht der Anwendung, die dynamischen Regeln wiederherzustellen.

Führen Sie die folgenden Schritte aus, bevor Sie die Komponente Firewall-Verwaltung aktivieren:

- Deaktivieren Sie andere Tools, die die Firewall des Betriebssystems verwalten.
- Speichern und sichern Sie alle benutzerdefinierten Firewall-Regeln, die vor der Aktivierung der Komponente Firewall-Verwaltung konfiguriert wurden.

So erstellen Sie eine Regel für Netzwerkpakete

Die Firewall filtert alle Netzwerkaktivitäten auf den geschützten Geräten gemäß den *Regeln für Netzwerkpakete*. Regeln für Netzwerkpakete beschränken Netzwerkpakete oder Verbindungen unabhängig von der Anwendung. Regeln erlauben oder verbieten Netzwerkaktivitäten gemäß den folgenden Bedingungen:

- Verbindungsprotokoll und Port
- Richtung des Datenverkehrs
- IP-Adresse des Geräts, das Netzwerkdatenverkehr sendet oder empfängt

Prioritäten von Regeln für Netzwerkpakete

Standardmäßig alle ausgehenden Pakete und Verbindungen. Standardregeln haben die niedrigste Priorität: Wenn keine andere Regel für Netzwerkpakete ausgelöst wurde oder keine anderen Regeln für Netzwerkpakete angegeben wurden, wird die Aktivität erlaubt.

Die Firewall wendet Regeln für Netzwerkpakete in der Reihenfolge ihrer Priorität an. Die Priorität einer Regel entspricht ihrer Position in der Liste von oben nach unten. Die Firewall filtert eine Netzwerkverbindung anhand der ersten Regel in der Liste und erlaubt oder blockiert die Netzwerkaktivität. Wenn die Regel nicht übereinstimmt, wendet die Firewall die nächste Regel an und fährt so in der Liste fort. Anschließend ignoriert die Komponente alle Regeln für Netzwerkpakete, die nach der für die Verbindung übereinstimmenden Regel stehen.

Empfehlungen zum Erstellen von Regeln für Netzwerkpakete

Über die Befehlszeile können Sie Regeln für Netzwerkpakete mithilfe von Befehlszeilenoptionen oder einer Konfigurationsdatei erstellen. Wenn Sie mehrere Regeln hinzufügen möchten, verwenden Sie dazu eine Konfigurationsdatei.

Das Hinzufügen einer großen Anzahl von Regeln nacheinander mithilfe von Befehlszeilenoptionen kann zu einem sprunghaften Anstieg der CPU-Auslastung führen.

So erstellen Sie eine Regel für Netzwerkpakete in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wählen Sie **Kommunikations- und Web-Schutz → Firewall**.

5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **Firewall AKTIVIERT** befindet.

6. Klicken Sie auf der Registerkarte **Regeln für Netzwerkpakete** auf **Hinzufügen**.

   Dadurch wird das Formular für eine neue Netzwerkregel geöffnet (siehe Abbildung unten).

7. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

   Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf den Link **Regelvorlage auswählen** klicken. Regelvorlagen enthalten Einstellungen für die am häufigsten verwendeten Netzwerkverbindungen.

   Alle Einstellungen einer Netzwerkregel, mit Ausnahme der Priorität und der Aktionen, die die Firewall auf die Verbindung anwendet, werden automatisch ausgefüllt.

8. Geben Sie im Feld **Priorität** die Priorität der Regel an. Standardmäßig wird eine Regel mit der höchsten Priorität erstellt.

9. Wählen Sie unter **Aktion** aus, wie die Firewall Netzwerkaktivitäten verarbeiten soll, wenn die Regel ausgelöst wird: **Erlauben** oder **Blockieren**.

10. Wählen Sie im Feld **Richtung** aus, für welche Netzwerkaktivitäten die Regel gelten soll:

    - **Eingehend**. Die Firewall wendet die Netzwerkregel auf alle eingehenden Netzwerkpakete an.
    - **Eingehend (Paket)**. Die Firewall wendet die Netzwerkregel auf alle Netzwerkpakete an, die über eine von einem Remote-Computer initiierte Verbindung gesendet werden.
    - **Eingehend/Ausgehend**. Die Firewall wendet diese Netzwerkregel sowohl auf eingehende als auch auf ausgehende Netzwerkpakete an. Dabei bleibt unberücksichtigt, ob die Netzwerkverbindung vom lokalen Computer oder von einem Remote-Computer initiiert wurde.
    - **Ausgehend (Paket)**. Die Firewall wendet die Netzwerkregel auf alle ausgehenden Netzwerkpakete an.
    - **Ausgehend**. Die Firewall wendet die Netzwerkregel auf alle Netzwerkpakete an, die über eine vom Benutzercomputer initiierte Verbindung gesendet werden.
    - **Eingehend / Ausgehend (Pakete)**. Die Firewall wendet die Netzwerkregel auf alle eingehenden und ausgehenden Netzwerkpakete an.

11. Aktivieren Sie das Kontrollkästchen **Ereignisse protokollieren**, damit die Aktionen der Netzwerkregel im Bericht aufgezeichnet werden. Gemäß der Aktion der Regel erstellt das Programm ein Ereignis vom Typ *Netzwerkaktivität verboten* oder *Netzwerkaktivität erlaubt*.

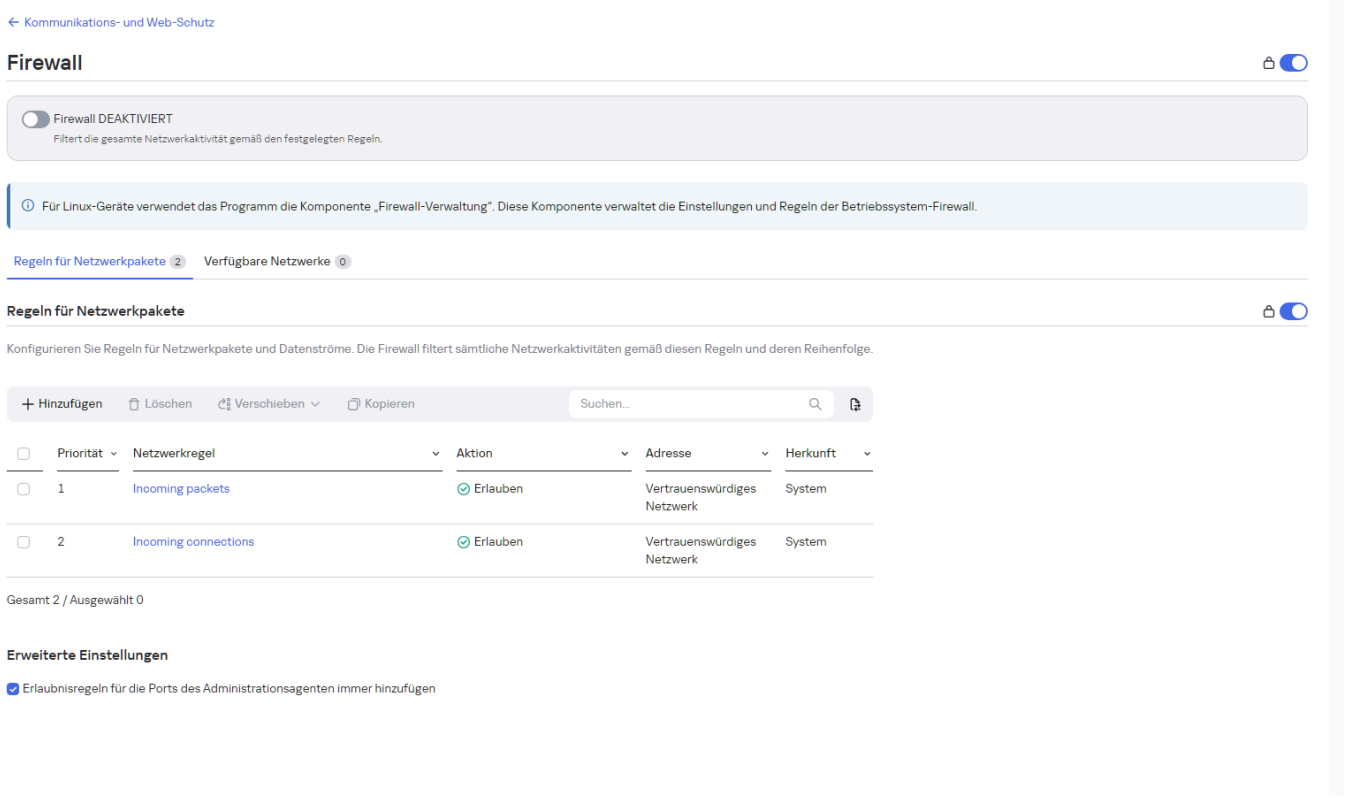
12. Wählen Sie auf der Registerkarte **Protokolleinstellungen** das Protokoll aus, nach dem die Regel Netzwerkaktivitäten filtern soll.

13. Gehen Sie zur Registerkarte **Remote-Netzwerkadressen**.

14. Geben Sie im Feld **Remote** die Netzwerkadressen der Remote-Computer an, die Netzwerkpakete senden und empfangen können: Die Firewall wendet die Regel auf die angegebenen Adressen an.

15. Geben Sie im Feld **Lokal** die Netzwerkadressen der Computer an, auf denen Kaspersky Endpoint Security installiert ist und die Netzwerkpakete senden und empfangen können: Die Firewall wendet die Regel auf die angegebenen Adressen an.

16. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Firewall.

So erstellen Sie eine Regel für Netzwerkpakete über die Befehlszeile

1. Stellen Sie sicher, dass die Firewall-Verwaltung aktiviert ist:

   ```
   kesl-control --get-task-state 12
   ```

   Die Komponente muss den Status **Gestartet** haben.

2. Wenn die Komponente deaktiviert ist, führen Sie den Befehl aus:

   ```
   kesl-control --start-task 12
   ```

3. Fügen Sie eine neue Regel für Netzwerkpakete hinzu:

   ```
   kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
   <direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
   ```

   Wenn Sie mehrere Regeln hinzufügen möchten, verwenden Sie dazu eine Konfigurationsdatei:

   a. Geben Sie die Einstellungen der Komponente in die Konfigurationsdatei aus:

   ```
   kesl-control --get-settings 12 --file <path to file> [--json]
   ```

b. Öffnen Sie die Konfigurationsdatei und fügen Sie Regeln für Netzwerkpakete mit den folgenden Abschnitten hinzu:

```
[PacketRules.item_#]
Name=<rule name>
FirewallAction=<Allow|Block>
Protocol=<protocol>
Direction=<direction>
RemoteAddress=<remote address>
LocalAddress=<local address>
LogAttempts=<Yes|No>
```

c. Importieren Sie die Einstellungen aus der Konfigurationsdatei in das Programm:

```
kesl-control --set-settings 12 --file <path to file> [--json]
```

4. Um die Liste der Regeln für Netzwerkpakete anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control -F --query
```

Das Programm zeigt eine Liste aller Regeln für Netzwerkpakete in folgendem Format an: `<IP protocol version> <table> <chain> <rule in the format of the iptables-save utility>`.

Symbole

Befehlsoptionen

Parameter	Description
`--name <rule name>` `Name`	Name der Netzwerkpaketregel Standardmäßig: `Packet rule #<n>`.
`--action` `FirewallAction`	Aktion, die mit den in dieser Netzwerkpaketregel angegebenen Verbindungen ausgeführt wird. • `Allow` (Standard), um Verbindungen zuzulassen. • `Block` (Standard), um Verbindungen zu blockieren.
`--protocol` `Protocol`	Protokolltyp, für den Sie die Netzwerkaktivität überwachen möchten. • `Any` (Standard) bedeutet, dass die Firewall die gesamte Netzwerkaktivität kontrolliert • `TCP` • `UDP` • `ICMP` • `ICMPv6` • `IGMP` • `GRE`
`--direction` `Direction`	Richtung der überwachten Netzwerkaktivität: • `IncomingOutgoing` oder `InOut` (Standard). Die Firewall wendet die Netzwerkregel auf alle eingehenden und ausgehenden Netzwerkpakete an. • `Incoming` oder `In`. Die Firewall wendet die Netzwerkregel auf alle Netzwerkpakete an, die über eine von einem Remote-Computer initiierte Verbindung gesendet werden. • `Outgoing` oder `Out`. Die Firewall wendet die Netzwerkregel auf alle Netzwerkpakete an, die über eine vom Benutzercomputer initiierte Verbindung gesendet werden. • `IncomingPacket` oder `InPacket`. Die Firewall wendet die Netzwerkregel auf alle eingehenden Netzwerkpakete an. • `OutgoingPacket` oder `OutPacket`. Die Firewall wendet die Netzwerkregel auf alle ausgehenden Netzwerkpakete an. • `IncomingOutgoingPacket` oder `InOutPacket`. Die Firewall wendet diese Netzwerkregel sowohl auf eingehende als auch auf ausgehende Netzwerkpakete an. Dabei bleibt unberücksichtigt, ob die Netzwerkverbindung vom lokalen Computer oder von einem Remote-Computer initiiert wurde.

Parameter	Description
`--remote <remote address[:<port>]>` `RemoteAddress=<remote address>`	IP-Adresse des Remote-Geräts: • `Any` (Standard) aktiviert die Überwachung von Netzwerkpaketen, die von Remote-Geräten mit beliebiger IP-Adresse gesendet und/oder empfangen werden. • `Trusted` ist die konfigurierte Netzwerkzone für vertrauenswürdige Netzwerke. • `Local` ist die konfigurierte Netzwerkzone für lokale Netzwerke. • `Public` ist die konfigurierte Netzwerkzone für öffentliche Netzwerke. • `d.d.d.d` ist die IPv4-Adresse, wobei d eine Dezimalzahl von 0 bis 255 ist. • `d.d.d.d – d.d.d.d` ist ein Bereich von IPv4-Adressen. • `d.d.d.d/p` ist ein IPv4-Subnetz, wobei `p` eine Zahl von 0 bis 32 ist. • `x:x:x:x:x:x:x:x` ist eine IPv6-Adresse, wobei x eine hexadezimale Zahl von 0 bis ffff ist. • `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` ist ein Bereich von IPv6-Adressen. • `x:x:x:x:x:x:x:x/p` ist ein Subnetz von IPv6-Adressen, wobei `p` eine Zahl von 0 bis 128 ist; der Kürze halber können Sie `::` verwenden. Sie können auch einen Remote-Port angeben: • `Any` (Standard), um alle Remote-Ports zu überwachen • `0 – 65535`.
`--local <local address[:<port>]>` `LocalAddress=<local address>`	Netzwerkadresse eines Geräts, auf dem Kaspersky Endpoint Security installiert ist: • `Any` (Standard), um Netzwerkpakete zu überwachen, die von lokalen Geräten mit beliebiger IP-Adresse gesendet und/oder empfangen werden. • `Trusted` ist die konfigurierte Netzwerkzone für vertrauenswürdige Netzwerke. • `Local` ist die konfigurierte Netzwerkzone für lokale Netzwerke. • `Public` ist die konfigurierte Netzwerkzone für öffentliche Netzwerke. • `d.d.d.d` ist die IPv4-Adresse, wobei d eine Dezimalzahl von 0 bis 255 ist. • `d.d.d.d – d.d.d.d` ist ein Bereich von IPv4-Adressen. • `d.d.d.d/p` ist ein IPv4-Subnetz, wobei `p` eine Zahl von 0 bis 32 ist. • `x:x:x:x:x:x:x:x` ist eine IPv6-Adresse, wobei x eine hexadezimale Zahl von 0 bis ffff ist. • `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` ist ein Bereich von IPv6-Adressen. • `x:x:x:x:x:x:x:x/p` ist ein Subnetz von IPv6-Adressen, wobei `p` eine Zahl von 0 bis 128 ist; der Kürze halber können Sie `::` verwenden. Sie können auch einen lokalen Port angeben: • `Any` (Standard), um alle lokalen Ports zu überwachen • `0 – 65535`.
`--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.
`LogAttempts`	Aktiviert das Protokollieren von Aktionen der Netzwerkregel im Bericht. • `Yes` – Aktionen im Bericht protokollieren. • `No` (Standardwert) – Aktionen nicht im Bericht protokollieren.

Beispiel für eine Regel, die alle eingehenden und bestehenden Verbindungen zum TCP-Port 23 blockiert

```
kesl-control -F --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --
remote any
```

Beispiel für eine Regel, die eingehende und bestehende Verbindungen über TCP-Port 23 für die öffentliche Netzwerkzone blockiert

```
kesl-control -F --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --
remote Public
```

Beispiele für die Verwendung von Regeln für Netzwerkpakete

1. **Internetzugriff nur für einen bestimmten Computer im lokalen Netzwerk erlauben und für alle anderen blockieren**

   Regel für einen Computer (192.168.2.22), dem der Internetzugriff über das TCP-Protokoll erlaubt ist:

   ```
   kesl-control --add-rule --name InternetAccess --action Allow --protocol TCP --local 192.168.2.22
   ```

   Regel für andere Computer, für die der Internetzugriff blockiert ist:

   ```
   kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.1.0/24
   ```

2. **Internetzugriff nur für einen bestimmten Computer im lokalen Netzwerk blockieren**

   Regel für den Computer (192.168.2.23), für den der Internetzugriff blockiert ist:

   ```
   kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.2.23
   ```

3. **Zugriff aus dem lokalen Netzwerk auf eine bestimmte Website blockieren**

   Regel für Computer im lokalen Netzwerk, denen der HTTP-Zugriff auf example.com (91.198.174.192) verweigert wird:

   ```
   kesl-control --add-rule --name ExampleHTTP --action Block --protocol TCP --remote 91.198.174.192:80
   ```

   Regel für Computer im lokalen Netzwerk, denen der HTTPS-Zugriff auf example.com (91.198.174.192) verweigert wird:

   ```
   kesl-control --add-rule --name ExampleHTTPS --action Block --protocol TCP --remote 91.198.174.192:443
   ```

4. **Einem bestimmten Computer im lokalen Netzwerk nur den Zugriff auf eine bestimmte Website erlauben**

   Regel für einen Computer (192.168.2.24), dem der HTTP-Zugriff auf example.com (91.198.174.192) erlaubt ist:

   ```
   kesl-control --add-rule --name ExampleHTTP --action Allow --protocol TCP --remote 91.198.174.192:80 --local
   192.168.2.24
   ```

   Regel für einen Computer (192.168.2.25), dem der HTTPS-Zugriff auf example.com (91.198.174.192) erlaubt ist:

   ```
   kesl-control --add-rule --name ExampleHTTPS --action Allow --protocol TCP --remote 91.198.174.192:443 --local
   192.168.2.25
   ```

   Regel für den Computer (192.168.2.26), die den Internetzugriff blockiert:

   ```
   kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.2.26
   ```

So fügen Sie einer Netzwerkzone eine IP-Adresse hinzu: Öffentlich, Lokal, Vertrauenswürdig

Die Firewall ermöglicht die Überwachung der Netzwerkaktivität für *Netzwerkzonen*. Eine Netzwerkzone ist eine Gruppe von IP-Adressen oder Subnetzen, die unter einem Typ der Netzwerkverbindung zusammengefasst sind. Sie können eine vordefinierte Netzwerkzone verwenden, um eine Regel für mehrere IP-Adressen oder Subnetze wiederzuverwenden, ohne für jede IP-Adresse oder jedes Subnetz eine separate Regel erstellen zu müssen.

Kaspersky Endpoint Security unterscheidet drei Netzwerkzonen:

- **Öffentliches Netzwerk**. Das Netzwerk wird durch Antiviren-Programme, Firewalls oder Filter geschützt (z. b. WLAN in einem Café). Für den Benutzer eines Computers, der mit einem solchen Netzwerk verbunden ist, blockiert die Firewall den Zugriff auf die Dateien und Drucker dieses Computers. Auch Drittnutzer erhalten über gemeinsame Ordner oder Fernzugriff keinen Zugang zu Informationen auf dem Desktop Ihres Computers.

- **Lokales Netzwerk**. Netzwerk für Benutzer, für die der Zugriff auf die Dateien und Drucker dieses Computers beschränkt ist (beispielsweise ein lokales Unternehmensnetzwerk oder ein privates Netzwerk).

- **Vertrauenswürdiges Netzwerk**. Sicheres Netzwerk, in dem einem Computer keine Angriffe und unerlaubte Zugriffsversuche auf Daten drohen. Für Netzwerke mit diesem Status erlaubt die Firewall jede beliebige Netzwerkaktivität innerhalb des Netzwerks.

So fügen Sie in der Web Console einer Netzwerkzone eine IP-Adresse hinzu

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie **Kommunikations- und Web-Schutz** → **Firewall**.
5. Gehen Sie zur Registerkarte **Verfügbare Netzwerke**.
6. Klicken Sie auf **Hinzufügen**.

   Dadurch wird das Formular zum Hinzufügen einer neuen Netzwerkverbindung geöffnet.
7. Tragen Sie im Feld **Name** den Namen der Netzwerkverbindung ein.
8. Wählen Sie im Feld **Netzwerktyp** die Netzwerkzone aus, zu der die Netzwerkverbindung gehört: **Öffentliches Netzwerk**, **Lokales Netzwerk**, **Vertrauenswürdiges Netzwerk**.
9. Geben Sie im Feld **IP-Adresse** die IP-Adresse oder das Subnetz an, die bzw. das der Netzwerkverbindung zugeordnet werden soll.
10. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So fügen Sie einer Netzwerkzone über die Befehlszeile eine IP-Adresse hinzu

1. Stellen Sie sicher, dass die Firewall-Verwaltung aktiviert ist:

   ```
   kesl-control --get-task-state 12
   ```

   Die Komponente muss den Status **Gestartet** haben.

2. Wenn die Komponente deaktiviert ist, führen Sie den Befehl aus:

   ```
   kesl-control --start-task 12
   ```

3. Fügen Sie die Adresse der Netzwerkzone hinzu:

   ```
   kesl-control -F --add-zone <Public|Local|Trusted> --address <IP address>
   ```

   Um die Liste der Netzwerkpaketregeln anzuzeigen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control -F --query
   ```

Symbole

Befehlsoptionen

Parameter	Description
`--add-zone`	Vordefinierte Netzwerkzone: • `Public`. Öffentliches Netzwerk. • `Local`. Lokales Netzwerk. • `Trusted`. Vertrauenswürdiges Netzwerk.
`--address`	Netzwerkadresse oder Subnetz.

Beispiel

```
kesl-control -F --add-zone Local --address 10.28.0.0/24
```

Was sind dynamische Regeln?

Kaspersky Endpoint Security ermöglicht das Hinzufügen oder Entfernen von *dynamischen Regeln* der Firewall, die das Programm für den ordnungsgemäßen Betrieb benötigt. Beispielsweise:

- Der Administrationsagent fügt dynamische Regeln hinzu, die Verbindungen mit Kaspersky Security Center zulassen.
- Die Komponente „Schutz vor Verschlüsselung“ fügt dynamische Regeln für das Abfangen des Datenverkehrs, der über die Dateiübertragungs- und Dateispeicherprotokolle NFS und SMB übertragen wird hinzu. Dadurch kann die Komponente den Netzwerkverkehr von Geräten blockieren, deren Aktionen vom Programm als bösartige Verschlüsselung interpretiert werden.
- 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 erstellt automatisch dynamische Regeln, die Programmkomponenten den Zugriff auf Netzwerkressourcen ermöglichen. 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. Das Programm stellt einen Satz dynamischer Regeln wieder her, wenn eine dieser Regeln gelöscht wird, z. B. mithilfe des Dienstprogramms iptables. Wenn der kesl-Prozess vom Watchdog-Server beendet wird, werden alle Verweise auf die Regelketten, die vom Programm während seiner Ausführung erstellt wurden (mit Ausnahme von kesl-bypass), aus iptables gelöscht.

Sie können den Satz dynamischer Regeln mit folgendem Befehl anzeigen:

```
kesl-control -F --query
```

Das Programm zeigt eine Liste aller Regeln für Netzwerkpakete in folgendem Format an: `<IP protocol version> <table> <chain> <rule in the format of the iptables-save utility>`. Dynamische Regeln werden in separate Ketten unterteilt: `kesl_input`, `kesl_output`, `kesl_prerouting`, `kesl_postrouting`, `kesl_forward`.

Sie können die Einstellungen dynamischer Regeln nicht verwalten.

Beispiel

```
ipv4 mangle kesl_output -p tcp -m tcp --dport 80 -m mark ! --mark 0x400/0x400 -m conntrack --ctdir ORIGINAL -m
addrtype ! --dst-type LOCAL -j MARK --set-xmark 0x100/0x100 tag WebAv
```

So erstellen Sie Regeln für die Verbindung mit Kaspersky Security Center

Der Administrationsagent wird für die Interaktion mit Kaspersky Security Center verwendet. Für eine dauerhafte Verbindung zwischen dem Administrationsagenten und Kaspersky Security Center müssen Sie Erlaubnisregeln für die Ports des Administrationsagenten hinzufügen. In diesem Fall können Sie die Firewall in der Konsole von Kaspersky Security Center per Fernzugriff konfigurieren, selbst wenn Sie die Firewall falsch konfigurieren und versehentlich alle Verbindungen blockieren.

Die Auswahl der Ports hängt von der Rolle des Computers ab (z. B. Verteilungspunkt). Weitere Informationen zu den Ports, die auf dem Computer geöffnet werden, finden Sie in der Hilfe zu Kaspersky Security Center.

So fügen Sie Erlaubnisregeln für den Administrationsagenten in der Web Console hinzu

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie **Kommunikations- und Web-Schutz** → **Firewall**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **Firewall AKTIVIERT** befindet.

6. Aktivieren Sie das Kontrollkästchen **Erlaubnisregeln für die Ports des Administrationsagenten immer hinzufügen**.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So fügen Sie Erlaubnisregeln für den Administrationsagenten über die Befehlszeile hinzu

1. Stellen Sie sicher, dass die Firewall-Verwaltung aktiviert ist:

   ```
   kesl-control --get-task-state 12
   ```

   Die Komponente muss den Status **Gestartet** haben.

2. Wenn die Komponente deaktiviert ist, führen Sie den Befehl aus:

   ```
   kesl-control --start-task 12
   ```

3. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control --set-settings 12 OpenNagentPorts=Yes
   ```

4. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --get-settings 12
   ```

Sicherheitskontrolle

Gerätekontrolle

Die *Gerätekontrolle* verwaltet den Zugriff von Benutzern auf Geräte, die auf dem Client-Gerät installiert oder mit diesem verbunden 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.

Funktionsweise der Gerätekontrolle

Standardmäßig ist die Komponente Gerätekontrolle mit den Standardeinstellungen aktiviert.

1. **Ein Benutzer versucht, auf das Gerät zuzugreifen**
2. **Die Gerätekontrolle verwaltet den Zugriff auf den folgenden Ebenen:**
   - **Gerätetyp** gemäß der Klassifizierung der Komponente "Gerätekontrolle" (z. B. Drucker, Wechseldatenträger,

CD-/DVD-Laufwerke). Auf jeden Gerätetyp kann einer der folgenden *Zugriffsmodi* angewendet werden:

- *Erlauben*, um den Zugriff auf Geräte dieses Typs zu erlauben.
- *Blockieren*: Zugriff auf Geräte dieses Typs blockieren.
- *Je nach Bus-Verbindung* – Erlaubt oder blockiert den Zugriff auf Geräte, abhängig vom Zugriffsmodus für den Bus, über den das Gerät verbunden ist.
- *Benutzerdefiniert*: Zugriff auf Geräte abhängig von den Gerätezugriffsregeln erlauben oder blockieren.
- *Nur lesen* – Erlaubt nur Lesezugriff auf Geräte des ausgewählten Typs. Das Schreiben ist verboten.

- **Verbindungsbus**. Ein *Verbindungsbus* ist eine Schnittstelle, über die Geräte eine Verbindung mit dem Client-Gerät herstellen, z. B. USB oder 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.

3. **Abschluss der Untersuchung**

   Wenn das Gerät, auf das der Benutzer zuzugreifen versucht, für diesen Benutzer kein vertrauenswürdiges Gerät ist oder der Benutzer gemäß dem Zugriffsmodus keine Berechtigung für den Zugriff auf das Gerät besitzt, blockiert das Programm für diesen Benutzer den Zugriff auf das Gerät.

   Der Benutzer kann eine Anfrage an den Administrator der Organisation senden, um eine irrtümliche Blockierung zu melden, wenn er der Ansicht ist, dass eine solche vorliegt, oder er kann vorübergehenden Zugriff auf das Gerät anfordern.

Wenn die Komponente "Gerätekontrolle" beendet wird, entsperrt die App den Zugriff auf gesperrte Geräte.

Gerätekontrolle konfigurieren

1. **Vertrauenswürdige Geräte konfigurieren**

   Vertrauenswürdige Geräte sind Geräte, auf die jene Benutzer, die in den Einstellungen eines vertrauenswürdigen Gerätes angegeben sind, jederzeit vollständigen Zugriff besitzen. Sie können einem einzelnen Benutzer, einer Benutzergruppe oder allen Benutzern der Organisation Zugriff auf vertrauenswürdige Geräte gewähren. Sie können beispielsweise den Zugriff auf bestimmte USB-Geräte oder nur auf USB-Laufwerke zuzulassen. In der Folge wird der Zugriff auf sämtliche andere USB-Geräte verweigert.

2. **Zugriffsmodus konfigurieren**

   Sie können für Gerätetypen und Verbindungsbusse den Zugriffsmodus konfigurieren. Standardmäßig ist für alle Gerätetypen der Zugriffsmodus *Abhängig vom Bus* ausgewählt. Für Verbindungsbusse ist der Zugriffsmodus *Erlauben* ausgewählt. Basierend auf diesen Einstellungen gewährt die Gerätekontrolle Benutzern vollen Zugriff auf alle Geräte.

3. **Zugriffsregeln konfigurieren**

   Für Speichergeräte (Festplatten, Wechseldatenträger, Diskettenlaufwerke und CD/DVD-Laufwerke) können Sie *Zugriffsregeln* konfigurieren.

4. **Nachrichtenvorlage konfigurieren**

   Bei Bedarf können Sie den Vorlagentext der Nachricht anpassen, mit der der Benutzer über blockierten Zugriff auf das Gerät oder einen verbotenen Vorgang mit dem Gerät benachrichtigt wird.

5. **Vorübergehenden Zugriff auf das Gerät konfigurieren**

   Erlauben Sie Benutzern bei Bedarf, vorübergehenden Zugriff auf ein blockiertes Gerät zu erhalten.

Besonderheiten und Einschränkungen

- Wenn die Gerätekontrolle zum ersten Mal aktiviert wird, generiert sie für alle erkannten Geräte mit bekanntem Geräte- oder Bustyp ein *Gerät erlaubt*-Ereignis. Bei nachfolgenden Ausführungen der Komponente werden keine Wiederholungsereignisse generiert, es sei denn, die Kontrolleinstellungen für diese Geräte wurden geändert.
- Systemlaufwerke werden von der Gerätekontrolle nicht blockiert. Wenn die Anwendung das Systemlaufwerk nicht automatisch erkennen kann, wird die Komponente Gerätekontrolle mit einem Fehler abgeschlossen.
- 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 und 6.8 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 Verzeichnissen nicht unterstützt.
- 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.
- Wenn in den allgemeinen Einstellungen der Anwendung das Blockieren des Zugriffs auf Dateien während der Untersuchung deaktiviert ist, kann der Zugriff auf Geräte mithilfe des Zugriffszeitplans für Geräte nicht blockiert werden.

So verwalten Sie die Liste der vertrauenswürdigen Geräte über die Befehlszeile

Die Liste der vertrauenswürdigen Geräte enthält Informationen über Geräte, auf die zugegriffen werden darf (für bestimmte Benutzer oder Gruppen).

Über die Befehlszeile können Sie die Liste der vertrauenswürdigen Geräte anzeigen, Geräte zur Liste hinzufügen und daraus entfernen sowie die Liste der vertrauenswürdigen Geräte aus einer Datei importieren.

Liste der vertrauenswürdigen Geräte anzeigen

```
kesl-control --trusted-devices --list
```

Gerät zur Liste der vertrauenswürdigen Geräte hinzufügen

```
kesl-control --trusted-devices --add <device id or mask>
```

wobei `<device id or mask>` die Geräte-ID oder die Geräte-ID-Maske ist.

```
Gerät aus der Liste der vertrauenswürdigen Geräte löschen

kesl-control --trusted-devices --delete <device id or mask>
```

wobei `<device id or mask>` die Geräte-ID oder die Geräte-ID-Maske ist.

```
Liste der vertrauenswürdigen Geräte aus einer Datei importieren

kesl-control --trusted-devices --merge|--add|--replace --file <file>
```

wobei:

- `--merge` – Vereinigt die Listen der vertrauenswürdigen Geräte beim Import. Wenn die aktuelle Liste und die importierte Liste Einträge für ein Gerät mit der gleichen ID enthalten, werden die Parameter des vorhandenen Eintrags geändert. Für Geräte, die sich noch nicht in der aktuellen Liste befinden, werden Einträge hinzugefügt.
- `--add` – Ergänzt die aktuelle Liste der vertrauenswürdigen Geräte beim Import. Es werden nur die Einträge für Geräte hinzugefügt, die zuvor nicht in der Liste enthalten waren.
- `--replace` – Ersetzt die aktuelle Liste der vertrauenswürdigen Geräte. Die bestehende Liste vertrauenswürdiger Geräte wird durch die importierte Liste ersetzt.
- `--file <file>` ist der vollständige Pfad zur JSON-Datei, aus der die Liste der vertrauenswürdigen Geräte importiert wird.

Zugriffsmodus für Geräte konfigurieren

Für jeden Gerätetyp (gemäß der Klassifizierung der Komponente Gerätekontrolle, z. B. Drucker, Wechseldatenträger, CD/DVD-Laufwerke) kann einer der folgenden *Zugriffsmodi* angewendet werden:

- *Erlauben*, um den Zugriff auf Geräte dieses Typs zu erlauben.
- *Blockieren*: Zugriff auf Geräte dieses Typs blockieren.
- *Je nach Bus-Verbindung* – Erlaubt oder blockiert den Zugriff auf Geräte, abhängig vom Zugriffsmodus für den Bus, über den das Gerät verbunden ist.
- *Benutzerdefiniert*: Zugriff auf Geräte abhängig von den Regeln für den Gerätezugriff erlauben oder blockieren. *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. Dieser Zugriffsmodus kann nur Geräten zugewiesen werden, die für das Speichern von Daten vorgesehen sind (Festplatten, Wechseldatenträger, Disketten, CD/DVD-Laufwerke).
- *Nur lesen* – Erlaubt nur Lesezugriff auf Geräte des ausgewählten Typs. Das Schreiben ist verboten. Dieser Zugriffsmodus kann nur Geräten zugewiesen werden, die für das Speichern von Daten vorgesehen sind (Festplatten, Wechseldatenträger, Disketten, CD/DVD-Laufwerke). Wenn das Gerät den Zugriffstyp „Nur Lesen“ aufweist und das vertrauenswürdige Gerät einem bestimmten Benutzer zugewiesen wird, wird der zugewiesene Benutzer ignoriert und das Gerät allen Benutzern für den Schreibzugriff zur Verfügung gestellt.

So konfigurieren Sie den Gerätezugriffsmodus für Gerätetypen in der Web Console

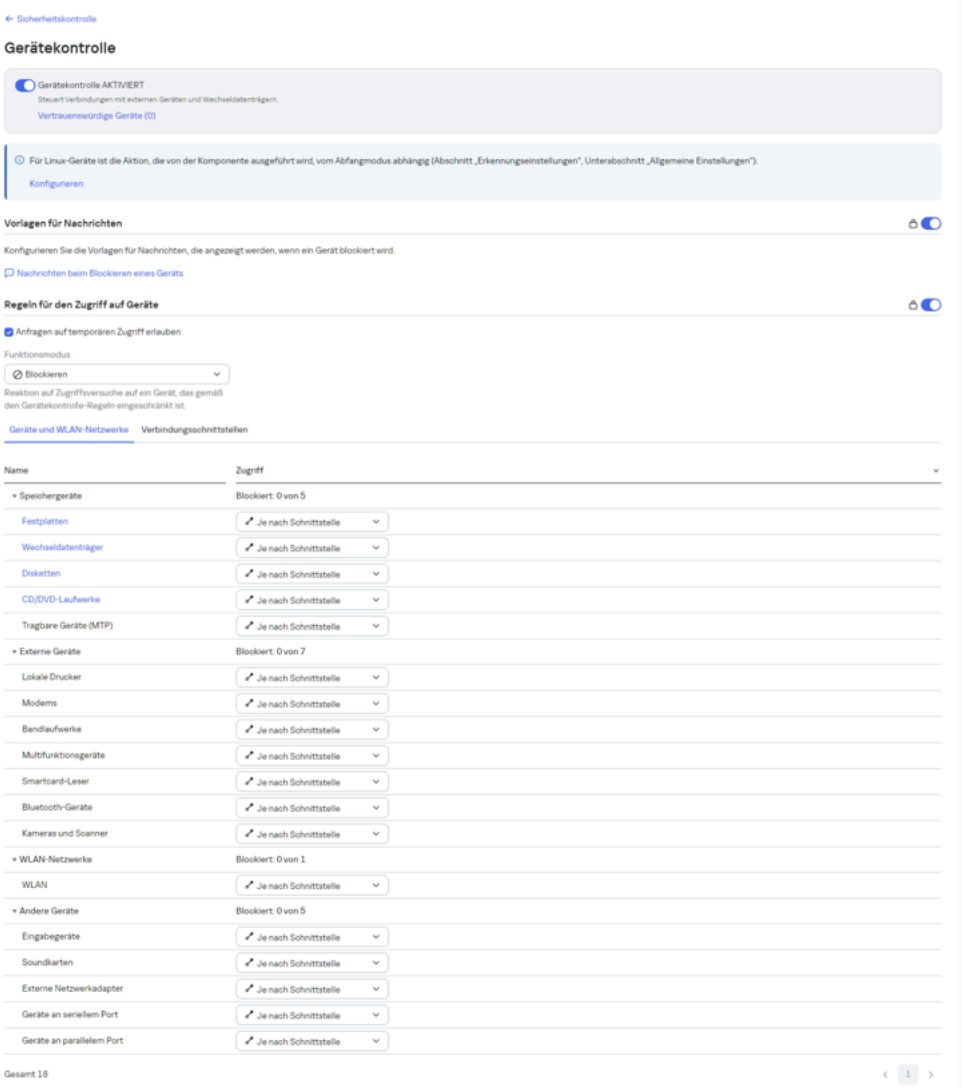
1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **Gerätekontrolle**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **Gerätekontrolle AKTIVIERT** befindet.
6. Wählen Sie unter **Regeln für den Zugriff auf Geräte** in der Tabelle die Registerkarte **Geräte und WLAN-Netzwerke** aus.
7. Wählen Sie in der Spalte **Name** den Gerätetyp aus, für den Sie den Zugriffsmodus konfigurieren möchten.
8. Wählen Sie in der Dropdown-Liste **Zugriff** einen der folgenden Zugriffsmodi aus:

   - **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.
   - **Benutzerdefiniert**: Zugriff auf Geräte abhängig von der Zugriffsregel und dem Zeitplan erlauben oder blockieren. Diese Option ist nur für Speichergeräte (Festplatten, Wechseldatenträger, Diskettenlaufwerke, CD/DVD-Laufwerke) verfügbar.
   - **Nur lesen** – Erlaubt nur Lesezugriff auf Geräte des ausgewählten Typs. Diese Option ist nur für Speichergeräte (Festplatten, Wechseldatenträger, Diskettenlaufwerke, CD/DVD-Laufwerke) verfügbar.
9. Klicken Sie in der Tabelle unten auf die Schaltfläche **Hinzufügen**.

   Dadurch wird ein Fenster zum Hinzufügen einer neuen Zugriffsregel geöffnet.
10. Legen Sie im Feld **Priorität** die Priorität der Zugriffsregel fest.
11. Wählen Sie die Benutzer oder die Benutzergruppe aus, für die die Zugriffsregel gelten soll. Standardmäßig gilt die Regel für alle Benutzer.
12. Legen Sie bei Bedarf einen Zugriffszeitplan fest. Die Regel wird standardmäßig immer angewendet.

13. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Gerätekontrolle

So konfigurieren Sie den Gerätezugriffsmodus für Gerätetypen über die Befehlszeile

1. Stellen Sie sicher, dass die Komponente Gerätekontrolle ausgeführt wird:

   ```
   kesl-control --get-task-list
   ```

   Die Komponente muss den Status **Gestartet** haben.

2. Wenn die Komponente deaktiviert ist, führen Sie den Befehl aus:

   ```
   kesl-control --start-task 15
   ```

3. Wählen Sie den Betriebsmodus beim Zugriffsversuch auf ein Gerät aus, das gemäß den Regeln der Gerätekontrolle eingeschränkt ist:

   ```
   kesl-control --set-settings 15 OperationMode=<Notify|Block>
   ```

4. Geben Sie den Zugriffsmodus für einen der Gerätetypen an: `HardDrive`, `RemovableDrive`, `FloppyDrive`, `OpticalDrive`, `SerialPortDevice`, `ParallelPortDevice`, `Printer`, `Modem`, `TapeDrive`, `MultifuncDevice`, `SmartCardReader`, `WiFiAdapter`, `NetworkAdapter`, `PortableDevice`, `PortableDevice`, `BluetoothDevice`, `ImagingDevice`, `SoundAdapter`, `InputDevice`

```
kesl-control --set-settings 15 DeviceClass.<device type>=<Allow|Block>
```

5. Um die Einstellungen der Gerätekontrolle anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 15
```

So konfigurieren Sie den Zugriffsmodus für den Verbindungsbus in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **Gerätekontrolle**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **Gerätekontrolle AKTIVIERT** befindet.
6. Wählen Sie unter **Regeln für den Zugriff auf Geräte** in der Tabelle die Registerkarte **Verbindungsschnittstellen** aus.
7. Wählen Sie in der Spalte **Name** den Bus aus, für den Sie den Zugriffsmodus konfigurieren möchten.
8. Wählen Sie in der Dropdown-Liste **Zugriff** einen der folgenden Zugriffsmodi aus:
   - **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.
9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie den Zugriffsmodus für den Verbindungsbus über die Befehlszeile

1. Stellen Sie sicher, dass die Komponente Gerätekontrolle ausgeführt wird:

```
kesl-control --get-task-list
```

   Die Komponente muss den Status **Gestartet** haben.
2. Wenn die Komponente deaktiviert ist, führen Sie den Befehl aus:

```
kesl-control --start-task 15
```

3. Wählen Sie den Betriebsmodus beim Zugriffsversuch auf ein Gerät aus, das gemäß den Regeln der Gerätekontrolle eingeschränkt ist:

```
kesl-control --set-settings 15 OperationMode=<Notify|Block>
```

4. Geben Sie den Zugriffsmodus für Verbindungsbusse an:

```
kesl-control --set-settings 15 DeviceBus.USB=<Allow|Block>
kesl-control --set-settings 15 DeviceBus.FireWire=<Allow|Block>
```

5. Um die Einstellungen der Gerätekontrolle anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 15
```

Gerätezugriffsregeln konfigurieren

Für Speichergeräte (Festplatten, Wechseldatenträger, Diskettenlaufwerke und CD/DVD-Laufwerke) können Sie Zugriffsregeln konfigurieren. *Eine Gerätezugriffsregel* ist 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. Dieser Zugriffsmodus kann nur Geräten zugewiesen werden, die für das Speichern von Daten vorgesehen sind (Festplatten, Wechseldatenträger, Disketten, CD/DVD-Laufwerke). Wenn ein Gerät, auf das der Zugriff verboten ist, angeschlossen wird, verweigert die Anwendung 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 Anwendung 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.

So konfigurieren Sie eine Gerätezugriffsregel in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **Gerätekontrolle**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **Gerätekontrolle AKTIVIERT** befindet.
6. Wählen Sie unter **Regeln für den Zugriff auf Geräte** in der Tabelle die Registerkarte **Geräte und WLAN-Netzwerke** aus.
7. Wählen Sie in der Spalte **Name** den Typ des Speichergeräts aus, für das Sie eine Zugriffsregel hinzufügen möchten (Festplatten, Wechseldatenträger, Diskettenlaufwerke, CD / DVD-Laufwerke).
8. Wählen Sie im folgenden Fenster unter **Regeln für den Zugriff auf Geräte** den Punkt **Benutzerdefiniert** aus.

9. Klicken Sie in der Tabelle unten auf die Schaltfläche **Hinzufügen**.

   Dadurch wird ein Fenster zum Hinzufügen einer neuen Zugriffsregel geöffnet.

10. Legen Sie im Feld **Priorität** die Priorität der Zugriffsregel fest.

11. Wählen Sie die Benutzer oder die Benutzergruppe aus, für die die Zugriffsregel gelten soll. Standardmäßig gilt die Regel für alle Benutzer.

12. Legen Sie bei Bedarf einen Zugriffszeitplan fest. Die Regel wird standardmäßig immer angewendet.

13. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie eine Gerätezugriffsregel über die Befehlszeile

1. Stellen Sie sicher, dass die Komponente Gerätekontrolle ausgeführt wird:

   ```
   kesl-control --get-task-list
   ```

   Die Komponente muss den Status **Gestartet** haben.

2. Wenn die Komponente deaktiviert ist, führen Sie den Befehl aus:

   ```
   kesl-control --start-task 15
   ```

3. Um die Einstellungen der Gerätekontrolle anzuzeigen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --get-settings 15
   ```

4. Wählen Sie den Betriebsmodus beim Zugriffsversuch auf ein Gerät aus, das gemäß den Regeln der Gerätekontrolle eingeschränkt ist:

   ```
   kesl-control --set-settings 15 OperationMode=<Notify|Block>
   ```

5. Fügen Sie eine neue Zugriffsregel für einen der folgenden Gerätetypen hinzu:
   `HardDrivePrincipals.item_#.AccessRules.item_#`,
   `RemovableDrivePrincipals.item_#.AccessRules.item_#`,
   `FloppyDrivePrincipals.item_#.AccessRules.item_#` oder
   `OpticalDrivePrincipals.item_#.AccessRules.item_#`.

   - Aktivieren Sie die Regel und geben Sie den Standardzeitplan an:

     ```
     kesl-control --set-settings 15
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.UseRule=Yes
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.ScheduleName=Default
     ```

     Beispiel

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.AccessRules.item_0001.UseRule=Yes
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.ScheduleName=Default
     ```

   - Legen Sie die Aktion der Gerätekontrolle fest, wenn die Regel ausgelöst wird:

     ```
     kesl-control --set-settings 15
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.Access=Allow|Block
     ```

     Beispiel

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.AccessRules.item_0001.UseRule=Yes
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.Access=Allow
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.ScheduleName=Default
     ```

   - Geben Sie bei Bedarf die Benutzer an, für die die Regel gelten soll:

     ```
     kesl-control --set-settings 15 <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.Principal=<Name>=
     <\Everyone|user name|@group name>
     ```

     Beispiel

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.Principal=\Everyone
     ```

   - Bearbeiten Sie bei Bedarf den Zeitplan der Regel:

     ```
     kesl-control --set-settings 15 Schedules.item_#.ScheduleName=<Name> Schedules.item_#.DaysHours=<All|day of
     the week|hour>
     ```

     Beispiel

     ```
     kesl-control --set-settings 15 Schedules.item_0001.ScheduleName=Default Schedules.item_0001.DaysHours=All
     ```

So konfigurieren Sie die Nachrichtenvorlage der Gerätekontrolle

Wenn ein Benutzer versucht, auf ein gesperrtes Gerät zuzugreifen, zeigt die Anwendung eine Benachrichtigung darüber an, dass der Zugriff auf das Gerät verweigert wurde oder der Vorgang mit dem Gerät untersagt ist.

Für die Benachrichtigung über verweigerten Zugriff wird eine Vorlage verwendet, in welcher die Ursachen für die Sperrung beschrieben werden. Für den Text der Vorlage können spezielle Variablen verwendet werden (z. B. %USER_NAME%). Durch die Variablen ist es möglich, eine einzige Benachrichtigungsvorlage für verschiedene Geräte zu verwenden. Beim Generieren einer Nachricht fügt die Anwendung die Werte von Variablen, die einem bestimmten Gerät, Benutzer und Ereignis entsprechen, in die Nachricht ein.

Sie können den Inhalt der Benachrichtigungsvorlage ändern.

So bearbeiten Sie die Nachrichtenvorlage in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **Gerätekontrolle**.
5. Klicken Sie unter **Vorlagen für Nachrichten** auf den Link **Nachrichten beim Blockieren eines Geräts**.

   Dadurch wird das Fenster zur Konfiguration der Nachrichtenvorlage geöffnet.
6. Konfigurieren Sie die Nachrichtenvorlage der Gerätekontrolle auf der Registerkarte **Nachricht an Benutzer**.
7. Über die Schaltflächen **Variable hinzufügen** und **Link hinzufügen** können Sie Variablen und Links zum Text der Benachrichtigung an den Benutzer hinzufügen. Um dem Vorlagentext eine Variable hinzuzufügen, platzieren Sie den Cursor an einer beliebigen Stelle im Text, klicken Sie auf die Schaltfläche **Variable hinzufügen** und wählen Sie die erforderliche Variable aus der Dropdown-Liste. Um dem Vorlagentext einen Link hinzuzufügen, platzieren Sie den Cursor an einer beliebigen Stelle im Text, klicken Sie auf die Schaltfläche **Link hinzufügen**.

   Wenn Sie den Text der Nachrichtenvorlage wiederherstellen möchten, klicken Sie auf die Schaltfläche **Standard wiederherstellen**.
8. Klicken Sie auf die Schaltfläche **OK**.
9. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

So ändern Sie eine Nachrichtenvorlage in der Verwaltungskonsole

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** → **Gerätekontrolle** aus.
5. Klicken Sie im Block **Vorlagen** auf die Schaltfläche **Anpassen**.
6. Konfigurieren Sie im neuen Fenster **Benachrichtigungsvorlagen** auf der Registerkarte **Nachricht bei blockiertem Vorgang** die Benachrichtigungsvorlage der Gerätekontrolle.

Über die Schaltflächen **Variable** und **Link** können Sie Variablen und Links zum Text der Benachrichtigung an den Benutzer hinzufügen. Um dem Vorlagentext eine Variable hinzuzufügen, platzieren Sie den Cursor an einer beliebigen Stelle im Text, klicken Sie auf die Schaltfläche **Variable** und wählen Sie die erforderliche Variable aus der Dropdown-Liste. Um dem Vorlagentext einen Link hinzuzufügen, platzieren Sie den Cursor an einer beliebigen Stelle im Text, klicken Sie auf die Schaltfläche **Link**.

Sie können außerdem den ursprünglichen Text der Benachrichtigungsvorlage wiederherstellen, indem Sie auf die Schaltfläche **Standard** klicken.

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

8. Klicken Sie auf **Übernehmen**.

Temporären Zugriff auf das Gerät gewähren

Bei der Konfiguration der Gerätekontrolle kann es versehentlich passieren, dass der Administrator den Zugriff auf ein Gerät sperrt, das ein Benutzer für seine Arbeit benötigt. Wenn der Benutzer der Ansicht ist, dass der Zugriff auf ein Gerät oder ein Vorgang mit dessen Inhalten irrtümlich gesperrt wurde, kann er beim lokalen Netzwerkadministrator der Organisation temporären Zugriff auf das gesperrte Gerät anfordern.

Der temporäre Zugriff kann angefordert werden, wenn der Administrator einen Benutzer dazu berechtigt hat. Der Administrator kann diese Berechtigung in den Richtlinieneigenschaften in der Web Console, in der Verwaltungskonsole oder in den Einstellungen der Aufgabe „Gerätekontrolle“ konfigurieren.

Das Gewähren des Zugriffs auf ein gesperrtes Gerät umfasst die folgenden Schritte:

1. Der Benutzer erstellt eine *Datei mit einer Zugriffsanfrage* und übergibt diese per E-Mail oder auf beliebige Weise an den Administrator (Der Administrator kann dies in der Benachrichtigungsvorlage über das Blockieren angeben). Der Benutzer kann temporären Zugriff auf das gesperrte Gerät über die grafische Benutzeroberfläche des Programms oder über die Befehlszeile anfordern.

2. Der Administrator generiert aus der Datei mit der Zugriffsanfrage einen *Zugriffsschlüssel* und sendet diesen per E-Mail oder auf beliebige Weise an den Benutzer. Der Zugriff auf ein gesperrtes Gerät wird in der Web Console gewährt.

3. Der Benutzer lädt den Zugriffsschlüssel hoch und erhält temporären Zugriff auf das gesperrte Gerät. Der Benutzer kann den Zugriffsschlüssel über die grafische Benutzeroberfläche oder über die Befehlszeile des Programms hochladen.

Das Gewähren von Zugriff auf ein blockiertes Gerät ist nur dann verfügbar, wenn in der Organisation die Lösung "Kaspersky Security Center 16.1" bereitgestellt ist und das Client-Gerät eine Verbindung mit dem Administrationsserver herstellen kann.

So erstellen Sie in der Web Console einen Zugriffsschlüssel für das gesperrte Gerät

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 mit dem gewünschten Gerät aus und aktivieren Sie das Kontrollkästchen neben dessen Namen.

3. Klicken Sie oberhalb der Liste der verwalteten Geräte auf die Schaltfläche **Offline-Zugriff auf Gerät gewähren**. Falls die Schaltfläche nicht sichtbar ist, klicken Sie auf die Schaltfläche mit den drei Punkten und wählen Sie im Menü **Offline-Zugriff auf Gerät gewähren**.

4. Klicken Sie im neuen Fenster **Anwendungseinstellungen** im Abschnitt **Gerätekontrolle** auf die Schaltfläche **Durchsuchen** und laden Sie die vom Benutzer erhaltene Zugriffsanfrage-Datei hoch.

   Es werden Informationen zum gesperrten Gerät angezeigt, für das der Benutzer Zugriff angefordert hat.

5. Ändern Sie gegebenenfalls im Feld **Zugriffsdauer** den Wert in Stunden.

   Standardmäßig ist das Feld **Zugriffsdauer** auf den Wert eingestellt, den der Benutzer beim Generieren der Zugriffsanfrage-Datei angegeben hat.

6. Ändern Sie bei Bedarf den Wert im Feld **Geben Sie den Zeitraum an, innerhalb dessen der Schlüssel für den Zugriff auf das Gerät gültig ist**.

   Dieses Feld enthält den Zeitraum, in dem der Benutzer den Zugriffsschlüssel herunterladen kann.

7. Klicken Sie auf die Schaltfläche **Schlüssel erstellen**.

8. Speichern Sie die Schlüsseldatei mit acode-Erweiterung.

So fordern Sie temporären Zugriff über die Befehlszeile an und erhalten ihn

Wenn der Benutzer der Ansicht ist, dass der Zugriff auf das Gerät versehentlich gesperrt oder ein Vorgang mit dem Inhalt des Geräts versehentlich untersagt wurde, kann der Benutzer beim Administrator des lokalen Netzwerks des Unternehmens temporären Zugriff auf das gesperrte Gerät mithilfe des folgenden Verwaltungsbefehls für die Gerätekontrolle anfordern:

Temporären Zugriff auf ein blockiertes Gerät anfordern

```
kesl-control --request-temporary-device-access --device-id <device identifier>  --access-duration <access
duration> --path <path to the access request file>
```

wobei:

`--device-id <device identifier>` ist die ID des gesperrten Geräts, auf das Sie zugreifen möchten.

`--access-duration <access duration>` ist der Zeitraum, für den Sie Zugriff auf das Gerät erhalten möchten (in Stunden). Mögliche Werte: 1 – 100.

`--path <path to the access request file>` ist der Pfad zu dem Verzeichnis, in dem Sie die Zugriffsanforderungsdatei mit der Erweiterung .akey speichern möchten.

Durch Ausführen des Befehls wird eine Zugriffsanfrage-Datei erstellt, die auf beliebige Weise (z. B. per E-Mail) dem Administrator übermittelt werden muss (der Administrator kann dies in der Nachrichtenvorlage über das Blockieren angeben).

Nachdem Sie den Zugriffsschlüssel vom Administrator erhalten haben, müssen Sie den Zugriffsschlüssel eingeben, um temporären Zugriff auf das Gerät zu erhalten.

Zugriffsschlüssel für ein blockiertes Gerät hochladen

```
kesl-control --upload-temporary-device-access-key --path <path to the file with the access key>
```

wobei:

`--path <path to the file with the access key>` ist der Pfad zur Datei mit dem Zugriffsschlüssel für das Gerät (Datei mit der Erweiterung .acode).

Der Befehl zeigt Informationen über die dem Gerät gewährten Zugriffsrechte und den Zeitraum an, für den diese Zugriffsrechte gelten.

So fordern Sie temporären Zugriff über die grafische Benutzeroberfläche an und erhalten ihn

Wenn Sie ein Gerät anschließen, auf das der Zugriff durch die Gerätekontrolle untersagt ist, öffnet sich ein Fenster mit der Meldung, dass der Zugriff auf das Gerät gesperrt ist.

Sie können über die grafische Benutzeroberfläche auf folgende Weise temporären Zugriff auf das gesperrte Gerät von Ihrem lokalen Netzwerkadministrator anfordern:

- Indem Sie im Fenster mit der Meldung über den gesperrten Gerätezugriff auf die Schaltfläche **OK** klicken.
- Über das Hauptfenster der grafischen Oberfläche der Anwendung.

So fragen Sie eine Erlaubnis für temporären Zugriff auf ein blockiertes Gerät an:

1. Öffnen Sie das Hauptfenster der grafischen Benutzeroberfläche des Programms.
2. Klicken Sie im unteren Bereich des Hauptfensters auf die Schaltfläche **Temporärer Zugriff**.

   Das Fenster **Temporärer Zugriff** wird geöffnet.

   Alternativ können Sie das Fenster **Temporärer Zugriff** auch im Fenster mit der Meldung über den gesperrten Gerätezugriff öffnen, indem Sie auf **OK** klicken.
3. Wählen Sie im Abschnitt **Zugriff auf ein gesperrtes Gerät anfordern** das gewünschte Gerät aus der Liste der verbundenen Geräte aus.
4. Geben Sie im Feld **Dauer des Zugriffs in Stunden** den gewünschten Zugriffszeitraum (in Stunden) an.
5. Klicken Sie auf die Schaltfläche **Zugriffsanfrage-Datei generieren**.
6. Geben Sie im sich öffnenden Fenster den Pfad zu dem Verzeichnis an, in dem die Zugriffsanfrage-Datei mit der akey-Erweiterung gespeichert werden soll.
7. Übergeben Sie die Datei mit der Zugriffsanfrage per E-Mail oder auf beliebige Weise an den Administrator (Der Administrator kann dies in der Benachrichtigungsvorlage über das Blockieren angeben).

Nachdem Sie vom Administrator einen Zugriffsschlüssel erhalten haben, können Sie diesen hochladen, um temporären Zugriff auf das gesperrte Gerät zu erhalten.

So erhalten Sie temporärem Zugriff auf ein blockiertes Gerät:

1. Öffnen Sie das Hauptfenster der grafischen Benutzeroberfläche des Programms.
2. Klicken Sie im unteren Bereich des Hauptfensters auf die Schaltfläche **Temporärer Zugriff**.

   Das Fenster **Temporärer Zugriff** wird geöffnet.
3. Klicken Sie im Abschnitt **Zugriff auf das Gerät erhalten** auf die Schaltfläche **Zugriffsschlüssel hochladen**.
4. Wählen Sie im sich öffnenden Fenster die Datei mit dem Zugriffsschlüssel für das Gerät (Datei mit acode-Erweitertung) aus, die Sie vom lokalen Netzwerkadministrator Ihrer Organisation erhalten haben.

5. Es öffnet sich ein Fenster mit Informationen zum Gerät, für das Zugriff gewährt wurde, und zum Zeitraum, für den dieser Zugriff gewährt wurde.

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

Web-Kontrolle

Die „Web-Kontrolle“ verwaltet den Zugriff durch Benutzer auf Webressourcen. Dadurch können Sie den Datenverkehrsverbrauch senken und die unangemessene Nutzung der Arbeitszeit reduzieren. 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.

Die Web-Kontrolle ermöglicht es, den Zugriff auf Webressourcen nach Inhaltskategorie und Datentyp einzuschränken sowie den Zugriff auf einzelne Websites zu blockieren. Sie können beispielsweise den Benutzerzugriff auf die Inhaltskategorie "Soziale Netzwerke" oder auf andere Kategorien beschränken. Das Programm bestimmt den Datentyp anhand des Dateiformats, nicht anhand der Erweiterung.

Funktionsweise der Web-Kontrolle

1. **Das Programm überprüft Anfragen an Webressourcen**

   Die Web-Kontrolle bestimmt die Inhaltskategorie und den Datentyp einer Website mithilfe der folgenden Technologien:

   - Antiviren-Datenbanken.
   - Cloud-Dienste von Kaspersky Security Network.
   - Die Technologie der heuristischen Analyse ermöglicht die Erkennung von Bedrohungen, die noch nicht in den Kaspersky-Datenbanken erfasst sind.

2. **Das Programm wendet Regeln an**

   Das Programm wendet die Regeln der Web-Kontrolle in der Reihenfolge ihrer Priorität an. Je niedriger die Prioritätsnummer, desto höher ist die Priorität der Regel. Wenn auf eine Website mehrere Regeln zutreffen, wendet die Web-Kontrolle die Regel mit der höchsten Priorität an.

   Beispielsweise könnte die App das Web-Portal eines Unternehmens als soziales Netzwerk definieren. Um den Zugriff auf soziale Netzwerke zu beschränken und Zugriff auf das Web-Portal des Unternehmens zu gewähren, erstellen Sie zwei Regeln: eine Verbotsregel für die Website-Kategorie „*Soziale Netzwerke*“ und eine Erlaubnisregel für das Unternehmens-Web-Portal. Die Zugriffsregel für das Web-Portal des Unternehmens sollte dabei eine höhere Priorität bekommen als die Zugriffsregel für soziale Netzwerke.

3. **Abschluss der Untersuchung**

   Wenn eine Regel den Zugriff auf eine Webressource blockiert, zeigt das Programm im Browser eine Meldung über die Blockierung an. Der Zugriff auf die Ressource wird gesperrt.

   Der Benutzer kann eine Anfrage bezüglich der irrtümlichen Blockierung an den Administrator der Organisation senden, wenn er der Meinung ist, dass die Webseite irrtümlich blockiert wurde.

Web-Kontrolle konfigurieren

1. **Regeln der Web-Kontrolle konfigurieren**

   Die Web-Kontrolle verwaltet den Zugriff von Benutzern auf Websites mithilfe von *Zugriffsregeln*. Mit diesen Regeln können Sie den Zugriff auf Websites für einzelne Benutzer einschränken und einen Zeitplan für den Zugriff konfigurieren.

   Beispielsweise können Sie den Zugriff auf Websites in der Kategorie *Kommunikation im Internet* für alle Benutzer in der Organisation außer der IT-Abteilung einschränken.

2. **Nachrichtenvorlagen konfigurieren**

   Je nach Aktion der Zugriffsregel zeigt die Web-Kontrolle dem Benutzer eine Meldung über den Besuch einer unerwünschten Website oder eine Meldung über die Blockierung an. Wenn eine Website blockiert wird, kann der Benutzer eine Nachricht bezüglich der irrtümlichen Blockierung an den Administrator des lokalen Netzwerks senden.

   Vorlagen werden für solche Nachrichten bereitgestellt.

   > Die Vorlagen können nicht über die Befehlszeile bearbeitet werden.

3. **Web-Kontrolle aktivieren**

   Die Web-Kontrolle ist standardmäßig deaktiviert. Aktivieren Sie die Komponente in der Web Console oder in der Verwaltungskonsole mithilfe des Schalters oder in der Befehlszeile mit dem folgenden Befehl:

   ```
   kesl-control --start-task 26
   ```

Besonderheiten und Einschränkungen

- Die App untersucht keine Dateien in Archiven. Wenn beispielsweise Bilddateien archiviert werden, erkennt die Anwendung den Datentyp als "Archive" und nicht als "Bilddateien".
- Kaspersky Endpoint Security überwacht nur HTTP- und HTTPS-Datenverkehr.
- Wenn der Schutz vor Web-Bedrohungen und die Web-Kontrolle gleichzeitig ausgeführt werden, werden die Einstellungen des Schutzes vor Web-Bedrohungen auf die Webressource angewendet. Das bedeutet, dass eine schädliche Website oder eine Phishing-Website blockiert wird, auch wenn die Regeln der Web-Kontrolle den Zugriff darauf erlauben.

So erstellen Sie eine Zugriffsregel für Webressourcen

Eine *Zugriffsregel für Webressourcen* ist eine Auswahl von Filtern und Aktionen, die Kaspersky Endpoint Security anwendet, wenn Benutzer Webressourcen besuchen. Zugriffsregeln können einen Zeitplan die Regel enthalten.

Regeln beschränken den Zugriff auf Webressourcen mithilfe der folgenden Filter:

- **Inhaltskategorien**. Die Web-Kontrolle kategorisiert Webressourcen nach Inhalt und Datentyp. Dadurch kann der Benutzerzugriff auf Websites mit einer bestimmten Inhaltskategorie (z. B. *Zahlungssysteme*) und/oder einem bestimmten Datentyp (z. B. *Ausführbare Dateien*) eingeschränkt werden.

- **Individuelle Websites**. Die Web-Kontrolle ermöglicht die Beschränkung des Benutzerzugriffs auf einzelne Adressen oder Adressgruppen von Webressourcen.

  Bei Domänen von Webadressen wird die Groß-/Kleinschreibung nicht berücksichtigt. Wenn eine Regel eine Webadresse wie `examPLE.com` enthält, beschränkt die Web-Kontrolle den Zugriff auf `example.com`.

  Wenn in einer Zugriffsregel gleichzeitig ein Filter nach Inhaltskategorie und ein Filter nach einzelnen Websites konfiguriert sind, beschränkt die Web-Kontrolle den Zugriff nicht auf alle Websites der angegebenen Inhaltskategorie, sondern nur auf die angegebenen Webadressen.

- **Filter nach Benutzername und Benutzergruppe**. Die Web-Kontrolle ermöglicht die Beschränkung des Zugriffs auf Webressourcen für einzelne Benutzer oder Benutzergruppen. Sie können beispielsweise den Zugriff auf Websites sozialer Medien für alle Benutzer im Unternehmen mit Ausnahme der IT-Abteilung einschränken.

- **Zeitplan der Regel**. Der Anwendungszeitplan der Regeln bestimmt den Zeitpunkt, an dem die App den Zugriff auf die in der Regel angegebenen Webressourcen kontrolliert. Sie können beispielsweise den Zugriff auf unerwünschte Websites nur während der Arbeitszeit beschränken.

Wenn gar keine Verbotsregel erstellt wurde, wird der HTTPS-Verkehr nicht entschlüsselt.

So erstellen Sie eine Zugriffsregel in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **Web-Kontrolle**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **Web-Kontrolle AKTIVIERT** befindet.
6. Wählen Sie unter **Regelliste** die Standardaktion der Web-Kontrolle aus:
   - **Alle erlauben, die nicht in der Regelliste angegeben sind**
   - **Alle blockieren, die nicht in der Regelliste angegeben sind**
7. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Dadurch wird das Formular zum Hinzufügen einer neuen Zugriffsregel geöffnet.
8. Geben Sie im Feld **Regelname** den Regelnamen ein. Der Relgename muss eindeutig sein.
9. Legen Sie im Feld **Priorität** die Priorität der Zugriffsregel fest.

10. Wählen Sie die Aktion aus, die die Web-Kontrolle auf Webressourcen anwenden soll, wenn die Regel ausgelöst wird:

    - **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. Durch Klicken auf die Links in der Blockierungsnachricht kann der Benutzer eine Nachricht an den lokalen Netzwerkadministrator senden, um die fälschliche Blockierung zu melden.

    - **Informieren**. Die Web-Kontrolle zeigt eine Warnung vor dem Besuch einer unerwünschten Webressource an. Wenn der Benutzer der Meinung ist, dass die Warnung falsch ist, kann er über den Link in der Warnung eine Webseite aufrufen oder eine Anfrage an den Administrator des lokalen Netzwerks des Unternehmens senden.

11. Wählen Sie einen Filter für die Zugriffsregel aus:

    - **Inhaltskategorien**. Geben Sie die Inhaltskategorien an, die von der Zugriffsregel kontrolliert werden sollen. Sie können mehrere Kategorien auswählen.

    - **Individuelle Websites**. Geben Sie eine Website-Adresse oder eine Gruppe von Websites an.

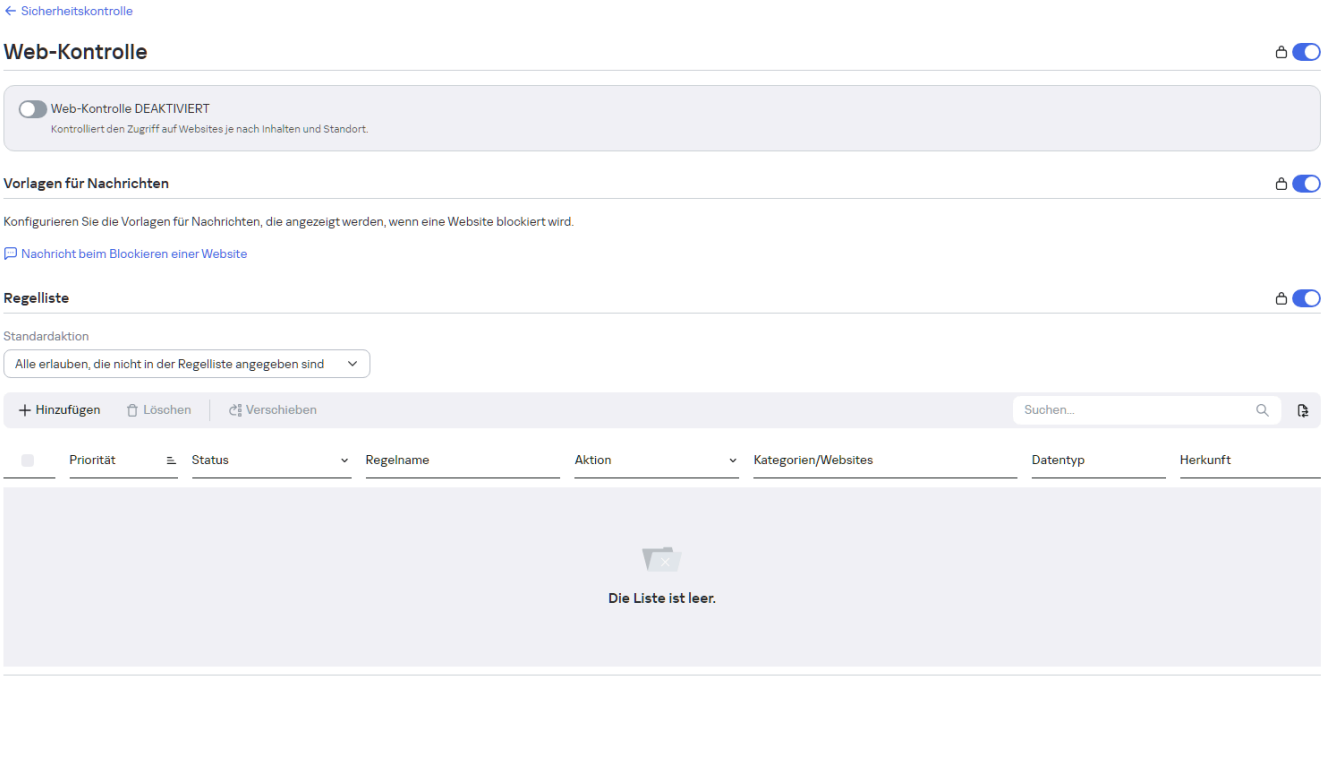
      In der Web Console können Sie nicht gleichzeitig einen Filter nach Inhaltskategorie und nach einzelnen Websites einrichten.

12. Geben Sie bei Bedarf die Datentypen an, die von der Anwendung gefiltert werden sollen.

13. Wählen Sie die Benutzer oder die Benutzergruppe aus, für die die Zugriffsregel gelten soll. Standardmäßig gilt die Regel für alle Benutzer.

14. Legen Sie bei Bedarf einen Zugriffszeitplan fest. Die Regel wird standardmäßig immer angewendet.

15. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Web-Kontrolle

So erstellen Sie eine Zugriffsregel über die Befehlszeile

1. Stellen Sie sicher, dass die Komponente Web-Kontrolle aktiviert ist:

   ```
   kesl-control --get-settings 26
   ```

   Die Komponente muss den Status **Gestartet** haben.

2. Wenn die Komponente deaktiviert ist, führen Sie den Befehl aus:

   ```
   kesl-control --start-task 26
   ```

3. Wählen Sie die Standardaktion für die Web-Kontrolle aus:

   ```
   kesl-control --set-settings 26 WebControlDefaultAction=<Allow|Block>
   ```

4. Fügen Sie eine neue Zugriffsregel mit der ID `#` hinzu:

   a. Aktivieren Sie die Regel:

   ```
   kesl-control --set-settings 26 Rules.item_#.Enabled=Yes
   ```

   b. Geben Sie den Regelnamen ein:

   ```
   kesl-control --set-settings 26 Rules.item_#.Name=<rule name>
   ```

c. Geben Sie die Aktion an, die die Web-Kontrolle auf Webressourcen anwenden soll, wenn die Regel ausgelöst wird:

```
kesl-control --set-settings 26 Rules.item_#.WebControlAction=<Allow|Block|Notify>
```

d. Wenn Sie Webressourcen nach Inhaltskategorie filtern müssen:

```
kesl-control --set-settings 26 Rules.item_#.UseCategories=<ContentOnly|FormatOnly|ContentAndFormat>
kesl-control --set-settings 26 Rules.item_#.ContentCategories.item_#.ContentCategory=<category>
[Rules.item_#.FormatCategories.item_#.FormatCategory=<format>]
```

e. Wenn Sie einzelne Webressourcen filtern müssen:

```
kesl-control --set-settings 26 Rules.item_#.UseUrls=Yes
kesl-control --set-settings 26 Rules.item_#.Urls.item_#=<web address>
```

f. Geben Sie bei Bedarf die Benutzer an, für die die Regel gelten soll:

```
kesl-control --set-settings 26 Rules.item_#.UsePrincipals=Yes
kesl-control --set-settings 26 Rules.item_#.Principals.item_#.Name=<user name|@group name>
```

g. Geben Sie bei Bedarf einen Zeitplan für die Regel an:

```
kesl-control --set-settings 26 Rules.item_#.Schedules.item_#.Id=<ID> Rules.item_#.Schedules.item_#.Name=
<schedule name> Rules.item_#.Schedules.item_#.DaysHours=<day of the week|hour>
```

5. Um die Liste der Regeln der Web-Kontrolle anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 26
```

Symbole

Befehlsoptionen

Parameter	Description
`WebControlDefaultAction`	Die Aktion, die die Web-Kontrolle auf Webressourcen anwendet, die in keiner Zugriffsregel angegeben sind.
`Enabled=Yes`	Aktivieren Sie die Zugriffsregel mit der ID `#`.
`Name`	Name der Regel. Der Relgename muss eindeutig sein.
`WebControlAction`	Die Aktion, die die Web-Kontrolle auf Webressourcen anwendet, wenn die Regel ausgelöst wird: `Allow` (Standardwert) – Gewährt Zugriff auf die Webressource. `Block` – Verbietet den Zugriff auf die Webressource. `Notify` – eine Warnung beim Besuch einer unerwünschten Webressource anzeigen. Mittels eines Links in der Warnmeldung kann der Benutzer auf die angeforderte Webressource zugreifen.
`UseCategories`	Verwendung von Filtern nach Inhaltskategorien und Datentypkategorien in der Regel: `None` (Standardwert) – Keine Inhaltsfilter für die Webressourcen anwenden. `ContentOnly` – Filter nach Inhaltskategorien in der Regel anwenden. `FormatOnly` – Filter nach Datentypkategorien in der Regel anwenden. `ContentAndFormat` – Filter nach Inhaltskategorien und nach Datentypkategorien in der Regel anwenden.

Parameter	Description
`ContentCategories.item_#.ContentCategory`	Inhaltskategorie.
`FormatCategories.item_#.FormatCategory`	Datentypkategorie: `Video` – Videodateien `Audio` – Audiodateien `OfficeDocument` – Dateien von Office-Anwendungen `Executable` – Ausführbare Dateien `Archives` – Archive `Images` – Bilder `Scripts` – Skripte
`UseUrls=Yes`	Verwendung einzelner Websites in einer Filterregel.
`Urls.item_#`	Adresse der Webressource, deren Zugriff durch die Regel verwaltet wird. Zum Angeben der Adressen der Webressourcen können Sie Masken verwenden.
`UsePrincipals=Yes`	Anwenden eines Filters nach Benutzern, für welche die Zugriffsregel für eine Webressource gelten soll.
`Principals.item_#.Name`	Der Benutzer oder die Benutzergruppe, für den bzw. die die Zugriffsregel für Webressourcen gilt: `<user name>` ist der Name des Benutzers, für den die Regel gilt. `@<group name>` ist der Name der Benutzergruppe, für die die Regel gilt.
`Schedules.item_#.Id`	Zeitplan-ID.
`Schedules.item_#.Name`	Gibt den Namen eines Zeitplans an.
`Schedules.item_#.DaysHours`	Gibt die Zeitintervalle für einen Zeitplan an: `<day of week>` ist der Wochentag. Sie können entweder die vollständigen Namen der Wochentage oder Abkürzungen verwenden (für Montag können Sie beispielsweise `Mo`, `Mon` oder `Monday` angeben). Als Wochentage können Sie Intervalle oder bestimmte Tage angeben. Die Woche beginnt am Sonntag. `<hour>` – Stunden [0:24]. Für Stunden können Sie nur Intervalle angeben.

So ändern Sie Nachrichtenvorlagen der Web-Kontrolle

Abhängig von der in der Zugriffsregel angegebenen Aktion zeigt die Web-Kontrolle dem Benutzer beim Versuch, auf Webressourcen zuzugreifen, eine Nachricht an (indem die Antwort des HTTP-Servers durch eine HTML-Seite mit einer Nachricht ersetzt wird):

- **Warnmeldung.** Die Nachricht, die dem Benutzer angezeigt wird, wenn er versucht, eine unerwünschte Ressource aufzurufen. Die App zeigt diese Nachricht an, wenn für die Regel die Aktion **Informieren** ausgewählt ist.

  Wenn der Benutzer der Meinung ist, dass die Warnung falsch ist, kann er über den Link in der Warnung eine Webseite aufrufen oder eine Anfrage an den Administrator des lokalen Netzwerks des Unternehmens senden.

- **Nachricht über blockierte Webressource** Die Nachricht, die dem Benutzer angezeigt wird, wenn eine unerwünschte Webressource blockiert wird. Die App zeigt diese Nachricht an, wenn für die Regel die Aktion **Blockieren** ausgewählt ist.

  Wenn ein Benutzer der Meinung ist, dass eine Webressource irrtümlich blockiert wurde, kann er über den Link in der Nachricht über die Blockierung der Webressource eine Anfrage an den Administrator des lokalen Netzwerks des Unternehmens senden.

Es werden Vorlagen für Warnungen, Nachrichten über die Blockierung einer Webressource und Anfragen an den Administrator des lokalen Netzwerks des Unternehmens bereitgestellt. Zum Erstellen von Nachrichtenvorlagen stehen spezielle Variablen zur Verfügung (z. B. `%USER_NAME%`). Wenn Sie Variablen verwenden, kann ein und dieselbe Nachrichtenvorlage für verschiedene Computer genutzt werden. Wenn eine Nachricht generiert wird, ruft Kaspersky Endpoint Security den Wert der Variablen aus den Betriebssystemeinstellungen ab und fügt ihn passend zum Computer, Benutzer und Ereignis in die Nachricht ein.

Die Vorlagen können nicht über die Befehlszeile bearbeitet werden.

So bearbeiten Sie die Nachrichtenvorlage in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **Web-Kontrolle**.
5. Klicken Sie unter **Vorlagen für Nachrichten** auf den Link **Nachricht beim Blockieren einer Website**.

   Dadurch wird das Fenster mit den Nachrichtenvorlagen geöffnet.
6. Konfigurieren Sie die Nachrichtenvorlagen der Web-Kontrolle:

   - **Warnung**. Die Vorlage für die Warnung, die dem Benutzer angezeigt wird, wenn er versucht, eine unerwünschte Ressource aufzurufen.
   - **Nachricht beim Blockieren**. Die Vorlage für die Nachricht, die angezeigt wird, wenn eine unerwünschte Webseite oder Website blockiert wird.
   - **Nachricht an den Administrator**. Vorlage für eine Nachricht an den Administrator. Wird verwendet, wenn der Benutzer der Meinung ist, dass die Webseite irrtümlich blockiert wurde. Nachdem der Benutzer Zugriff angefordert hat, sendet die App ein *Nachricht an den Administrator über Zugriffsverbot auf Webseite*-Ereignis 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 Anwendung eine Nachricht an die angegebene E-Mail-Adresse des Administrators.

   Wenn Sie den Text der Nachrichtenvorlage wiederherstellen möchten, klicken Sie auf die Schaltfläche **Auf Standard-Text zurücksetzen**.
7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So ändern Sie eine Nachrichtenvorlage in der Verwaltungskonsole

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>**.

   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 Block **Vorlagen** 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 Vorlage für die Meldung, die erscheint, 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 Verwaltungskonsole 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 Anwendung eine Nachricht an die angegebene E-Mail-Adresse des Administrators.

   Auf den Registerkarten **Warnung** und **Nachricht bei blockiertem Vorgang** können Sie mittels der Schaltflächen **Variable** und **Link** Variablen und Links in den Text der Nachricht an den Benutzer einfügen.

   Sie können den ursprünglichen Text der Nachrichtenvorlage wiederherstellen, indem Sie auf die Schaltfläche **Standard** klicken.

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

8. Klicken Sie auf **Übernehmen**.

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` – die Domänenmaske `*.` stimmt mit `pictures.` überein.
   - `http://user.pictures.example.com` – die Domänenmaske `*.` stimmt mit `pictures.` und `user.` überein.
   - `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 einer Adressmaske wird wie `/*` oder als leere Zeile 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.

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 6
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.

Programmkontrolle

Die Programmkontrolle verwaltet den Start von Programmen von Drittanbietern auf Benutzergeräten. Dies verringert das Risiko einer Infektion des geschützten Geräts mit Malware.

Um die Komponente nutzen zu können, benötigen Sie eine Lizenz, in der diese Funktionalität enthalten ist.

Funktionsweise der Programmkontrolle

1. **Benutzer versucht, ein Programm von einem Drittanbieter auszuführen**
2. **Die Programmkontrolle wendet Regeln an**

   Die Programmkontrolle wendet nacheinander Regeln auf das zu startende Programm an. Je nach ausgewähltem Regelmodus *kontrolliert* die Komponente den Start von Programmen oder *testet* Regeln. Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel.

3 Abschluss der Untersuchung

Wenn die Regeln die Ausführung des Programms verhindern, blockiert die Komponente den Start dieses Programms und generiert ein *Programmstart verboten*-Ereignis. Im Testmodus blockiert die Komponente den Start dieses Programms nicht und generiert das *Programmstart im Testmodus verboten*-Ereignis.

Programmkontrolle anpassen

1 Inventarisierung von Programmen durchführen

Verwenden Sie die Aufgabe Inventarisierung, um eine Liste der Programme abzurufen, die auf den geschützten Geräten installiert sind. Erstellen Sie anhand dieser Informationen eine Liste der Programme, deren Ausführung Sie verhindern möchten.

2 Betriebsmodus der Programmkontrolle auswählen

Die Komponente "Programmkontrolle" kann in einem von zwei Modi ausgeführt werden:

- *Alle erlauben, die nicht in der Regelliste angegeben sind*. Die Programmkontrolle erlaubt Benutzern, beliebige Programme von Drittanbietern auszuführen, mit Ausnahme der Programme, die durch die Regeln verboten sind.
- *Alle blockieren, die nicht in der Regelliste angegeben sind*. Die Programmkontrolle erlaubt Benutzern, beliebige Programme von Drittanbietern auszuführen, mit Ausnahme der Programme, die erlaubt und durch die Regeln nicht verboten sind.

Die Wahl des Modus der Programmkontrolle hängt von der Sicherheitsrichtlinie Ihres Unternehmens sowie davon ab, wie viele Programme Sie kontrollieren möchten.

3 Programmkategorien erstellen

Definieren Sie Kategorien für erlaubte oder verbotene Programme. Die Programmkategorien gelten unabhängig von den Administrationsgruppen für alle Geräte im Unternehmensnetzwerk. Mit Programmkategorien können Sie Regeln für eine Gruppe von Programmen konfigurieren, anstatt diese anhand von Einschluss- und Ausnahmebedingungen zu konfigurieren.

Es wird empfohlen, die Kategorie „Programme für die Arbeit“ zu erstellen und eine Standardauswahl von Programmen in diese Kategorie aufzunehmen, die im Unternehmen eingesetzt werden. Falls bestimmte Benutzergruppen unterschiedliche Programmsets einsetzen, können Sie für jede Benutzergruppe eine separate Programmkategorie erstellen.

> Wir empfehlen, Programmkategorien in Kaspersky Security Center zu konfigurieren.

4 Regeln der Programmkontrolle konfigurieren

Die Komponente kontrolliert den Start von Programmen anhand von *Regeln der Programmkontrolle*, die Bedingungen definieren, unter denen die Programmkontrolle den Start eines Programms von Drittanbietern für eine ausgewählte Benutzergruppe erlaubt oder verweigert.

5 Regeln der Programmkontrolle testen

Standardmäßig ist die Programmkontrolle deaktiviert. Wir empfehlen, die Programmkontrolle im Testmodus zu aktivieren und die erstellten Regeln der Programmkontrolle zu testen. Das Programm blockiert die Ausführung von Programmen von Drittanbietern nicht, sendet jedoch Benachrichtigungen über deren Start an den Administrationsserver.

6 **Erfahren Sie, wie die Regeln der Programmkontrolle funktionieren**

Sehen Sie sich den Bericht über den Betrieb der Programmkontrolle im Testmodus an. Passen Sie nach dem Überprüfen der Informationen Ihre Regeln der Programmkontrolle nach Bedarf an.

7 **Verwendung der Regeln der Programmkontrolle aktivieren**

In diesem Modus verhindert Kaspersky Endpoint Security die Ausführung von Programmen von Drittanbietern, wenn die Regeln den Start dieser Programme nicht erlauben.

So aktivieren Sie die Verwendung der Regeln der Programmkontrolle in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **App-Kontrolle**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **App-Kontrolle AKTIVIERT** befindet.
6. Wählen Sie unter **Aktion beim Starten von Programmen** die Aktion **Regeln anwenden** für die Programmkontrolle aus.
7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren Sie die Verwendung der Regeln der Programmkontrolle über die Befehlszeile

Um den Testmodus für die Programmkontrolle auszuwählen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 21 AppControlRulesAction=ApplyRules
```

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 Aufgabe "App-Kontrolle" verbieten oder erlauben.

Besonderheiten und Einschränkungen

- Die App-Kontrolle unterstützt keine Startsteuerung für die Apps Snap, Flatpak und AppImage.
- 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 die Ausführung des Interpreters erlauben, blockiert die Programmkontrolle ein Skript, das von diesem Interpreter gestartet wurde, nicht. Wenn die Ausführung von mindestens einem der in der Befehlszeile des Interpreters angegebenen Skripte durch die Regeln verboten ist, blockiert Kaspersky Endpoint Security alle Skripte, die in der Befehlszeile des Interpreters angegeben sind. Ausnahme: cat script.py | python.

Programminventarisierung

Um optimale Regeln der Programmkontrolle zu erstellen, sollte zunächst bekannt sein, welche Programme auf geschützten Geräten im lokalen Unternehmensnetzwerk verwendet werden. Mithilfe der Aufgabe *Inventarisierung* können Sie folgende Informationen abrufen:

- Name und Version des Drittanbieter-Programms
- Eine kurze Beschreibung

Um die Aufgabe nutzen zu können, benötigen Sie eine Lizenz, in der diese Funktionalität enthalten ist.

In der Datenbank der Anwendung Kaspersky Security Center können Informationen über 150.000 verarbeitete Dateien gespeichert werden. Sobald das Limit erreicht ist, werden neue Dateien nicht mehr verarbeitet. Um die Inventarisierung fortzusetzen, müssen Sie auf dem geschützten Gerät die Dateien löschen, die während der vorherigen Inventarisierung zur Datenbank von Kaspersky Security Center hinzugefügt wurden.

Konfigurieren und Ausführen der Aufgabe „Inventarisierung“

1. **Erstellen einer Aufgabe „Inventarisierung“**

   So erstellen Sie eine Aufgabe „Inventarisierung“ in der Web Console

   1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

      Die Aufgabenliste wird geöffnet.

   2. Klicken Sie auf **Hinzufügen**.

      Der Assistent für neue Aufgaben wird gestartet.

   3. Passen Sie die Einstellungen der Aufgabe an:

      a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Linux 12.5**.

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

      c. Geben Sie im Feld **Aufgabenname** den Aufgabennamen ein.

      d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

   4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe.

   5. Schließen Sie den Assistenten ab.

   So erstellen Sie eine Aufgabe „Inventarisierung“ über die Befehlszeile

Um eine Aufgabe zu erstellen, führen Sie den folgenden Befehl aus:

```
kesl-control --create-task <task name> --type InventoryScan
```

wobei `<task name>` der Name der neuen Aufgabe ist.

Dieser Befehl gibt die ID der erstellten Aufgabe zurück.

Beispiel für das Ergebnis der Befehlsausführung:

Aufgabe erstellt (Aufgaben-ID: 100)

2 **Inventarisierungsbereiche konfigurieren**

Damit die Aufgabe gestartet werden kann, muss mindestens ein Inventarisierungsbereich festgelegt sein. Standardmäßig ist der Bereich *Ausführbare Befehle* – `/usr/bin` festgelegt.

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.

So konfigurieren Sie einen Inventarisierungsbereich in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die erstellte Aufgabe zur Inventarisierung.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wechseln Sie zum Abschnitt **Inventarisierungsbereiche**.

5. Klicken Sie auf **Hinzufügen**.

   Daraufhin wird das Fenster zum Hinzufügen von Inventarisierungsbereichen geöffnet.

6. Geben Sie im Feld **Name des Bereichs** einen Namen für den Inventarisierungsbereich ein, z. B. *Dateien auf dem Desktop*.

7. Geben Sie im Feld **Pfad** den Pfad zu einer einzelnen Datei oder einem Verzeichnis an, zum Beispiel `/path/to/folder`. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

8. Geben Sie bei Bedarf Masken für Objektnamen im Format der Befehlsshell an, zum Beispiel `*.txt`, `file?.*`. Fügen Sie Masken einzeln hinzu.

9. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie einen Inventarisierungsbereich über die Befehlszeile

1. Führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings <task name | task ID> ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. Um die aktuellen Einstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings <task name | task ID>
```

Symbole

Einstellungen der Inventarisierungsaufgabe

Parameter	Description
`UseScanArea=Yes`	Aktivieren eines Inventarisierungsbereichs mit der ID `#`. Sie können die Untersuchung eines Inventarisierungsbereichs vorübergehend deaktivieren, anstatt den Bereich zu löschen. Legen Sie dazu `ScanScope.item_#.UseScanArea=No` fest.
`AreaDesc`	Beschreibung des Inventarisierungsbereichs. Die maximale Länge einer Zeichenfolge, die mit dieser Einstellung angegeben werden kann, beträgt 4096 Zeichen.
`AreaMask.item_#`	Einschränkung des Inventarisierungsbereichs. Im Inventarisierungsbereich untersucht das Programm nur Objekte, die mittels Masken im Shell-Format angegeben wurden. Sie können mehrere Elemente vom Typ `ScanScope.item_#.AreaMask.item_#` in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge. Beispiel: `ScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Pfad zum Verzeichnis mit untersuchten Objekten. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske. Der Standardwert ist `/usr/bin`

3 Bearbeiten Sie bei Bedarf die Aufgabeneinstellungen

So konfigurieren Sie die Inventarisierungsaufgabe in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die erstellte Aufgabe zur Inventarisierung.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wechseln Sie zum Abschnitt **Inventarisierungseinstellungen**.

5. Wählen Sie eine Aktion für die Programmkategorie „Goldenes Image“ aus:

   - **Keine Änderungen** – die Kategorie „Goldenes Image“ nach Abschluss der Inventarisierung nicht ändern. Diese Option ist standardmäßig ausgewählt. Diese Option wird verwendet, wenn Sie eine Liste der auf dem Gerät verwendeten Programme von Drittanbietern abrufen möchten, diese jedoch nicht zur Kategorie „Golden Image“ hinzufügen möchten.

   - **Aktualisieren oder erstellen (falls nicht vorhanden)** – Programme, die durch die Inventarisierungsaufgabe auf dem Gerät erkannt wurden, zur Kategorie "Goldene Kategorie" hinzufügen. Wenn die Kategorie nicht vorhanden ist, wird sie erstellt. Wenn eine Kategorie existiert, wird die Liste der darin enthaltenen Anwendungen aktualisiert.

   - **Entfernen** – die Programmkategorie „Goldenes Image“ leeren. Die Kategorie wird sofort nach dem Start der Aufgabe geleert, ohne dass eine Inventarisierung der Dateien auf dem Gerät durchgeführt wird.

6. Aktivieren Sie bei Bedarf die folgenden Kontrollkästchen:

   - **Inventarisierung von Skriptdateien**. Auf Skripte im Inventarisierungsbereich prüfen. Das Programm sendet diese Informationen an Kaspersky Security Center.
   - **Alle ausführbaren Dateien untersuchen**.
   - **Binärdateien untersuchen**. Untersuchung von Binärdateien (Dateien mit den Erweiterungen .elf, .java und .pyc).

7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Inventarisierungsaufgabe über die Befehlszeile

Führen Sie den Befehl aus:

```
kesl-control --set-settings <task name | task ID> ScanScripts=<Yes|No> ScanBinaries=<Yes|No>
ScanAllExecutable=<Yes|No> GoldenImageAction=<DoNothing|Create|Remove>
```

Symbole

Einstellungen der Inventarisierungsaufgabe

Parameter	Description
`ScanScripts`	Prüfung auf Skripte im Inventarisierungsbereich: `Yes` (Standardwert) – Skripte untersuchen. `No` – Skripte nicht untersuchen.
`ScanBinaries`	Untersuchung von Binärdateien (Dateien mit den Erweiterungen .elf, .java und .pyc): `Yes` (Standardwert) – Binärdateien untersuchen. `No` – Binärdateien nicht untersuchen.
`ScanAllExecutable`	Untersuchung von ausführbaren Dateien: `Yes` (Standardwert) – Dateien mit Executable Bit untersuchen. `No` – Dateien mit Executable Bit nicht untersuchen.
`GoldenImageAction`	Die Aktion, die Kaspersky Endpoint Security nach Abschluss der Inventarisierungsaufgabe mit der Programmkategorie „Goldene Kategorie“ ausführen muss: `DoNothing` (Standard) – die Programmkategorie „Goldenes Image“ nicht ändern. `Create` – Erkannte Anwendungen werden zur Programmkategorie "Golden Image" hinzufügt. Wenn die Kategorie nicht vorhanden ist, wird sie erstellt. Wenn eine Kategorie existiert, wird die Liste der darin enthaltenen Anwendungen aktualisiert. `Remove` – die Programmkategorie „Goldene Kategorie“ leeren. Die Kategorie wird sofort nach dem Start der Aufgabe geleert, ohne dass eine Inventarisierung der Dateien auf dem Gerät durchgeführt wird.

4 Ausschlussbereich anpassen

Eine Ausnahme hat eine höhere Priorität als ein Inventarisierungsbereich. Ein ausgenommenes Objekt wird nicht untersucht, selbst wenn es sich in einem Inventarisierungsbereich befindet. Wenn der Inventarisierungsbereich auf einer niedrigeren Ebene als das ausgenommene Verzeichnis definiert ist, überspringt das Programm diesen Inventarisierungsbereich bei der Ausführung der Aufgabe.

So konfigurieren Sie einen Ausnahmebereich in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.
2. Die Aufgabenliste wird geöffnet.
3. Klicken Sie auf die erstellte Aufgabe zur Inventarisierung.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

4. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

5. Wechseln Sie zum Abschnitt **Ausschlussbereiche**.

6. Klicken Sie auf **Hinzufügen**.

   Das Fenster zum Hinzufügen von Ausnahmebereichen wird geöffnet.

7. Geben Sie im Feld **Name des Bereichs** den Namen des Ausnahmebereichs an, z. B. *Systemdateien*.

8. Geben Sie im Feld **Pfad** den Pfad zu einer einzelnen Datei oder einem Verzeichnis an (z. B. `/path/to/folder`). Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

9. Geben Sie Masken für Objektnamen im Format der Befehlsshell an (z. B. `*.txt` oder `file?.*`). Fügen Sie Masken einzeln hinzu.

10. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie einen Ausnahmebereich über die Befehlszeile

1. Führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings <task name | task ID>       ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. Um die aktuellen Einstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings <task name | task ID>
```

Symbole

Einstellungen der Inventarisierungsaufgabe

Parameter	Description
`UseScanArea`	Schließt den angegebenen Bereich von der Inventarisierung aus. Sie können einen Ausnahmebereich vorübergehend deaktivieren, anstatt den Bereich zu löschen. Legen Sie dazu `ExcludedFromScanScope.item_#.UseScanArea=No` fest.
`AreaDesc`	Beschreibung des von der Inventarisierung ausgeschlossenen Bereichs.
`AreaMask.item_#`	Einschränkung des Ausnahmebereichs. Im Ausnahmebereich nimmt die Anwendung nur die Objekte von Untersuchungen aus, die mithilfe von Masken im Shell-Format angegeben wurden. Sie können mehrere Elemente vom Typ `ExcludedFromScanScope.item_#.AreaMask.item_#` in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge. Beispiel: `ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Pfad zum Verzeichnis, das von der Inventarisierung ausgenommen werden soll. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

Beispiel für den Ausschluss des Verzeichnisses `/tmp` von der Inventarisierung:

```
kesl-control --set-settings 100 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

5 Aufgabe ausführen

So führen Sie die Aufgabe zur Inventarisierung in der Web Console aus

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.
   Die Aufgabenliste wird geöffnet.
2. Aktivieren Sie das Kontrollkästchen neben der erstellten Aufgabe.
3. Klicken Sie auf die Schaltfläche **Starten**.

So führen Sie eine Aufgabe zur Inventarisierung über die Befehlszeile aus

Um die Aufgabe auszuführen, führen Sie den folgenden Befehl aus:

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

wobei:

- `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `[-W]` – Gibt die aktuellen Ereignisse mit Bezug auf diese Aufgabe aus.
- `[--progress]` – Aktiviert das Anzeigen des Ausführungsfortschritts der Aufgabe.

Liste der gefundenen Apps anzeigen

Um die Liste der auf den Geräten gefundenen Apps in der Web Console anzuzeigen:

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.
   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf die erstellte Aufgabe zur Inventarisierung.
   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Ergebnisse** aus.

```
Liste der auf dem Client-Gerät erkannten Programme anzeigen
```

```
kesl-control --get-app-list [--json]
```

Kaspersky Endpoint Security zeigt für gefundene Apps die folgenden Informationen an:

- Datum und Uhrzeit der Inventarisierung
- Anzahl der Programme
- Liste der Apps mit folgenden Informationen:
  - Pfad zur Anwendung.
  - Hash-Summe der Anwendung.

- Typ der App. Zum Beispiel: `Script`, `Executable`.
- Kategorien, zu denen das Programm gehört (falls sie zuvor erstellt wurden). Sie können die Liste der erstellten App-Kategorien mit dem folgenden Befehl anzeigen:

```
kesl-control --get-categories
```

Wenn Sie eine neue Kategorie hinzufügen, werden deren Informationen in der Liste der Apps nicht automatisch aktualisiert. Um die Liste der Programme zu aktualisieren, müssen Sie die Inventarisierungsaufgabe erneut ausführen.

So konfigurieren Sie den Betriebsmodus der Programmkontrolle

Die Komponente "Programmkontrolle" kann in einem von zwei Modi ausgeführt werden:

- *Alle erlauben, die nicht in der Regelliste angegeben sind*. Die Programmkontrolle erlaubt Benutzern, beliebige Programme von Drittanbietern auszuführen, mit Ausnahme der Programme, die durch die Regeln verboten sind.
- *Alle blockieren, die nicht in der Regelliste angegeben sind*. Die Programmkontrolle erlaubt Benutzern, beliebige Programme von Drittanbietern auszuführen, mit Ausnahme der Programme, die erlaubt und durch die Regeln nicht verboten sind.

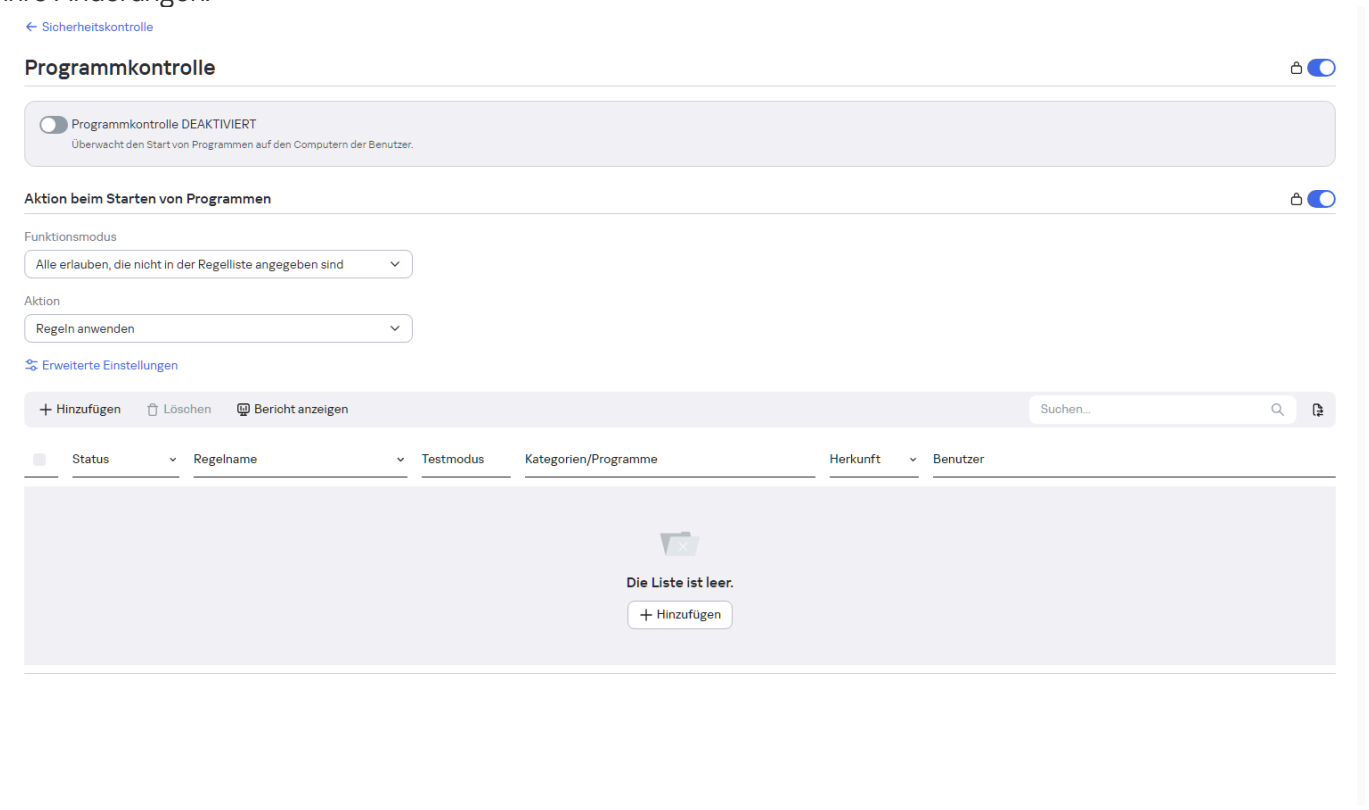
Die Wahl des Modus der Programmkontrolle hängt von der Sicherheitsrichtlinie Ihres Unternehmens sowie davon ab, wie viele Programme Sie kontrollieren möchten.

So passen Sie den Betriebsmodus der Programmkontrolle in der Web Console an

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **App-Kontrolle**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **App-Kontrolle AKTIVIERT** befindet.
6. Wählen Sie unter **Aktion beim Starten von Programmen** den Betriebsmodus der Programmkontrolle aus:
   - **Alle erlauben, die nicht in der Regelliste angegeben sind**
   - **Alle blockieren, die nicht in der Regelliste angegeben sind**

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Programmkontrolle

So passen Sie den Betriebsmodus der Programmkontrolle über die Befehlszeile an

Führen Sie den Befehl aus:

```
kesl-control --set-settings 21 AppControlMode=<AllowList|DenyList>
```

Symbole

Befehlsoptionen

Parameter	Description
`AppControlMode`	`AllowList` – Kaspersky Endpoint Security verbietet allen Benutzern den Start aller Anwendungen, außer der in den Regeln für die Programmkontrolle angegebenen. `DenyList` (Standardwert) – Kaspersky Endpoint Security erlaubt allen Benutzern den Start aller Anwendungen, außer der in den Regeln für die Programmkontrolle angegebenen.

Programmkategorien erstellen

Um das Anlegen von Regeln der Programmkontrolle zu vereinfachen, können Sie *Programmkategorien* erstellen.

Kaspersky Endpoint Security bestimmt die Kategorie eines Programms mithilfe der folgenden Technologien:

- Antiviren-Datenbanken.
- Cloud-Dienste von Kaspersky Security Network.
- Die Technologie der heuristischen Analyse ermöglicht die Erkennung von Bedrohungen, die noch nicht in den Kaspersky-Datenbanken erfasst sind.

In Kaspersky Endpoint Security für Linux können Kategorien basierend auf den folgenden Parametern erstellt werden:

- Name der ausführbaren App-Datei
- Name des Verzeichnisses mit der ausführbaren Anwendungsdatei.
- Hash der ausführbaren Anwendungsdatei Es ist nur SHA256 zulässig.

  Um Datei- und Verzeichnisnamen anzugeben, können Sie Masken verwenden.

  Regeln für die Angabe von Masken

  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. Beispielsweise `/dir/*/file*/` oder `/dir/file*/`.

  Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.

Es wird empfohlen, die Kategorie „Programme für die Arbeit“ zu erstellen und eine Standardauswahl von Programmen in diese Kategorie aufzunehmen, die im Unternehmen eingesetzt werden. Falls bestimmte Benutzergruppen unterschiedliche Programmsets einsetzen, können Sie für jede Benutzergruppe eine separate Programmkategorie erstellen.

Kaspersky Endpoint Security für Linux unterstützt keine KL-Kategorien.

Um in Kaspersky Security Center eine Programmkategorie zu erstellen:

1. Klicken Sie im Web Console-Hauptfenster auf **Asset-Verwaltung** → **Drittanbieteranwendungen** → **Programmkategorien**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent zum Erstellen einer benutzerdefinierten Kategorie wird gestartet.
3. Folgen Sie den Anweisungen des Assistenten zum Erstellen einer benutzerdefinierten Kategorie.

Schritt 1.

Geben Sie bei diesem Schritt den Namen der Programmkategorie an und wählen Sie einen Typ für die Programmkategorie aus:

- *Manuell zu erweiternde Kategorie. Informationen über ausführbare Dateien werden zur Kategorie manuell hinzugefügt*. Wenn Sie diesen Kategorietyp ausgewählt haben, können Sie bei den Schritten *Bedingungen* und *Ausnahmen* die Kriterien festlegen, nach denen ausführbare Dateien in die Kategorie aufgenommen werden sollen.

- *Kategorie für ausführbare Dateien aus einem bestimmten Ordner. Ausführbare Dateien von Anwendungen, die sich in dem angegebenen Ordner befinden, werden automatisch verarbeitet und deren Metriken werden zur Kategorie hinzugefügt*. Wenn Sie diesen Kategorietyp ausgewählt haben, können Sie im nächsten Schritt einen Ordner angeben, aus dem ausführbare Dateien automatisch in die Kategorie aufgenommen werden.

- *Kategorie für ausführbare Dateien von ausgewählten Geräten. Diese ausführbaren Dateien werden automatisch verarbeitet und deren Metriken werden zur Kategorie hinzugefügt*. Wenn Sie diesen Kategorietyp ausgewählt haben, können Sie beim nächsten Schritt einen Computer angeben, dessen ausführbare Dateien automatisch in diese Kategorie aufgenommen werden sollen.

Schritt 2.

Dieser Schritt ist verfügbar, wenn Sie den folgenden Kategorietyp ausgewählt haben: **Manuell zu erweiternde Kategorie. Informationen über ausführbare Dateien werden zur Kategorie manuell hinzugefügt**.

Wählen Sie bei diesem Schritt die Kriterien aus, nach denen Programme in die Kategorie aufgenommen werden sollen:

- **Aus der KL-Kategorie**

  Wenn diese Option ausgewählt ist, kann eine Kaspersky-Programmkategorie als Bedingung verwendet werden, um Programme zu der benutzerdefinierten Kategorie hinzuzufügen. Eine *KL-Kategorie* ist eine Liste von Programmen, die gemeinsame Themenattribute haben. Die Liste wird von Kaspersky-Experten geführt. Zur KL-Kategorie „Office-Programme“ gehören beispielsweise Programme aus den Paketen Microsoft Office, Adobe Acrobat und anderen.

  Sie können alle KL-Kategorien auswählen, um eine erweiterte Liste mit vertrauenswürdigen Programme zu erstellen.

- **Zertifikat aus Datenverwaltung auswählen**

  Wenn diese Option ausgewählt ist, können Sie Zertifikate aus dem Speicher angeben. Die Bedingung der Kategorie entspricht nur ausführbaren Dateien, die mit dem angegebenen Zertifikat signiert sind.

  Wenn Sie ein Zertifikat als Auslösebedingung für eine Regel ausgewählt haben, stellen Sie sicher, dass dieses Zertifikat dem vertrauenswürdigen Systemspeicher auf dem Computer hinzugefügt wurde, und überprüfen Sie die Programmeinstellungen für die Nutzung des vertrauenswürdigen Systemspeichers.

- **Pfad der Anwendung festlegen (Masken unterstützt)**

  Wenn diese Option ausgewählt ist, können Sie eine Datei oder einen Ordner auf dem Client-Gerät angeben, aus der bzw. dem ausführbare Dateien zu der benutzerdefinierten Programmkategorie hinzugefügt werden sollen. Sie können reguläre Ausdrücke verwenden (z. B. `C:\path_to_exe\*` oder `C:\Program Files\Internet Explorer\*`).

- **Wechseldatenträger**

  Wenn diese Option ausgewählt ist, können Sie den Typ des Datenträgers (beliebiger Datenträger oder Wechseldatenträger) angeben, von dem das Programm gestartet werden soll. Programme, die von einem Datenträger des ausgewählten Typs gestartet wurden, werden zu der benutzerdefinierten Programmkategorie hinzugefügt.

- **Hash, Metadaten oder Zertifikat**:

  - **Aus der Liste für ausführbare Dateien auswählen**

    Wenn diese Option ausgewählt ist, können Sie aus der Liste der ausführbaren Dateien auf dem Client-Gerät Programme auswählen, die zu der Kategorie hinzugefügt werden sollen.

  - **Aus der Registrierung für Programme auswählen**

    Wenn diese Option ausgewählt ist, wird die Registrierung für Programme angezeigt. Nachdem Sie ein Programm aus der Registrierung ausgewählt haben, wird ein Fenster geöffnet. Dort sind die Metadaten des ausgewählten Programms bereits eingetragen:

    - Dateiname
    - Dateiversion Sie können eine exakte Version festlegen oder eine Bedingung eingeben (z. B. „höher als 5.0“).
    - Anwendungsname.
    - Programmversion Sie können eine exakte Version festlegen oder eine Bedingung eingeben (z. B. „höher als 5.0“).
    - Hersteller.

    Bitte beachten: Es werden nur ausführbare Dateien blockiert, die den angegebenen Parametern entsprechen. Der Start des ausgewählten Programms wird dagegen nicht blockiert. Wenn die ausgewählten Metadaten mit den Metadaten der ausführbaren Datei übereinstimmen, die beim Start des Programms gestartet wird, können Sie zum nächsten Schritt gehen. Andernfalls müssen Sie die Werte manuell bearbeiten, damit sie mit den Metadaten der ausführbaren Datei übereinstimmen.

  - **Manuell festlegen**

    Wenn diese Option ausgewählt ist, müssen Sie als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie einen Datei-Hash, Metadaten oder ein Zertifikat angeben.

    Datei-Hash

    Abhängig von der Version des Sicherheitsprogramms, das auf den Geräten in Ihrem Netzwerk installiert ist, müssen Sie einen Hash-Algorithmus auswählen, den Kaspersky Endpoint Security auf Dateien dieser Kategorie anwenden soll. Informationen über die Hash-Werte, die durch Hash-Funktionen berechnet wurden, sind in der Datenbank des Administrationsservers gespeichert.

SHA256 ist eine kryptografische Hash-Funktion, deren Algorithmus keine bekannten Schwächen aufweist. Sie gilt derzeit als die sicherste Hash-Funktion. SHA256 wird von Kaspersky Endpoint Security 10 und höher unterstützt. Die MD5-Hash-Funktion wird für ältere Versionen als Kaspersky Endpoint Security 10 unterstützt.

Wählen Sie eine der Hash-Funktionen aus, die Kaspersky Endpoint Security auf Dateien der folgenden Kategorie anwenden soll:

- Wenn in Ihrem Netzwerk keine anderen Exemplare von Sicherheitsprogrammen installiert sind als Kaspersky Endpoint Security Version 10 oder höhere Versionen, aktivieren Sie das Kontrollkästchen **SHA256**. Es wird davor gewarnt, eine Kategorie auf Basis des SHA256-Hashs einer ausführbaren Datei für Kaspersky Endpoint Security 10 oder älter zu erstellen. Dies kann dazu führen, dass das Sicherheitsprogramm fehlerhaft funktioniert. In diesem Fall können Sie für Dateien dieser Kategorie die kryptografische MD5-Hash-Funktion verwenden.

- Wenn in Ihrem Netzwerk ältere Versionen als Kaspersky Endpoint Security 10 installiert sind, aktivieren Sie das Kontrollkästchen **MD5-Hash**. Für Kaspersky Endpoint Security 10 oder höher ist es nicht möglich, eine Kategorie auf Basis des MD5-Hashs einer ausführbaren Datei hinzuzufügen. In diesem Fall können Sie für Dateien dieser Kategorie die kryptografische SHA256-Hash-Funktion verwenden.

- Wenn es in Ihrem Netzwerk Geräte gibt, die sowohl ältere als auch neuere Versionen als Kaspersky Endpoint Security 10 verwenden, aktivieren Sie beide Kontrollkästchen: **SHA256** und **MD5-Hash**.

Metadaten

Wenn diese Option ausgewählt ist, können Sie Metadaten wie Dateiname, Dateiversion und Hersteller angeben. Die Bedingung der Kategorie entspricht nur ausführbaren Dateien mit identischen Metadaten.

Zertifikat

Wenn diese Option ausgewählt ist, können Sie Zertifikate aus dem Speicher angeben. Die Bedingung der Kategorie entspricht nur ausführbaren Dateien, die mit dem angegebenen Zertifikat signiert sind.

- **Aus einem MSI-Paket/Archivordner**

  Wenn diese Option ausgewählt ist, können Sie eine MSI-Installationsdatei als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie angeben. Die Metadaten des Installationsprogramms werden an den Administrationsserver gesendet. Programme, deren Installationsprogramm-Metadaten mit dem angegebenen MSI-Installationsprogramm übereinstimmen, werden zur benutzerdefinierten Programmkategorie hinzugefügt.

Schritt 3.

Dieser Schritt ist verfügbar, wenn Sie den folgenden Kategorietyp ausgewählt haben: **Manuell zu erweiternde Kategorie. Informationen über ausführbare Dateien werden zur Kategorie manuell hinzugefügt**.

Die Programme, die bei diesem Schritt angegeben werden, werden auch dann aus der Kategorie ausgeschlossen, wenn diese Programme beim Schritt „Legen Sie die Bedingungen für die Aufnahme der Programme in die Kategorie fest“ angegeben wurden.

Wählen Sie bei diesem Schritt die Kriterien aus, nach denen Programme aus der Kategorie ausgeschlossen werden sollen:

- **Aus der KL-Kategorie**

  Wenn diese Option ausgewählt ist, kann eine Kaspersky-Programmkategorie als Bedingung verwendet werden, um Programme zu der benutzerdefinierten Kategorie hinzuzufügen. Eine *KL-Kategorie* ist eine Liste von Programmen, die gemeinsame Themenattribute haben. Die Liste wird von Kaspersky-Experten geführt. Zur KL-Kategorie „Office-Programme“ gehören beispielsweise Programme aus den Paketen Microsoft Office, Adobe Acrobat und anderen.

  Sie können alle KL-Kategorien auswählen, um eine erweiterte Liste mit vertrauenswürdigen Programme zu erstellen.

- **Zertifikat aus Datenverwaltung auswählen**

  Wenn diese Option ausgewählt ist, können Sie Zertifikate aus dem Speicher angeben. Die Bedingung der Kategorie entspricht nur ausführbaren Dateien, die mit dem angegebenen Zertifikat signiert sind.

  Wenn Sie ein Zertifikat als Auslösebedingung für eine Regel ausgewählt haben, stellen Sie sicher, dass dieses Zertifikat dem vertrauenswürdigen Systemspeicher auf dem Computer hinzugefügt wurde, und überprüfen Sie die Programmeinstellungen für die Nutzung des vertrauenswürdigen Systemspeichers.

- **Pfad der Anwendung festlegen (Masken unterstützt)**

  Wenn diese Option ausgewählt ist, können Sie eine Datei oder einen Ordner auf dem Client-Gerät angeben, aus der bzw. dem ausführbare Dateien zu der benutzerdefinierten Programmkategorie hinzugefügt werden sollen. Sie können reguläre Ausdrücke verwenden (z. B. `C:\path_to_exe\*` oder `C:\Program Files\Internet Explorer\*`).

- **Wechseldatenträger**

  Wenn diese Option ausgewählt ist, können Sie den Typ des Datenträgers (beliebiger Datenträger oder Wechseldatenträger) angeben, von dem das Programm gestartet werden soll. Programme, die von einem Datenträger des ausgewählten Typs gestartet wurden, werden zu der benutzerdefinierten Programmkategorie hinzugefügt.

- **Hash, Metadaten oder Zertifikat**:

  - **Aus der Liste für ausführbare Dateien auswählen**

    Wenn diese Option ausgewählt ist, können Sie aus der Liste der ausführbaren Dateien auf dem Client-Gerät Programme auswählen, die zu der Kategorie hinzugefügt werden sollen.

  - **Aus der Registrierung für Programme auswählen**

    Wenn diese Option ausgewählt ist, wird die Registrierung für Programme angezeigt. Nachdem Sie ein Programm aus der Registrierung ausgewählt haben, wird ein Fenster geöffnet. Dort sind die Metadaten des ausgewählten Programms bereits eingetragen:

    - Dateiname
    - Dateiversion Sie können eine exakte Version festlegen oder eine Bedingung eingeben (z. B. „höher als 5.0“).
    - Anwendungsname.

- Programmversion Sie können eine exakte Version festlegen oder eine Bedingung eingeben (z. B. „höher als 5.0“).

- Hersteller.

Bitte beachten: Es werden nur ausführbare Dateien blockiert, die den angegebenen Parametern entsprechen. Der Start des ausgewählten Programms wird dagegen nicht blockiert. Wenn die ausgewählten Metadaten mit den Metadaten der ausführbaren Datei übereinstimmen, die beim Start des Programms gestartet wird, können Sie zum nächsten Schritt gehen. Andernfalls müssen Sie die Werte manuell bearbeiten, damit sie mit den Metadaten der ausführbaren Datei übereinstimmen.

- **Manuell festlegen**

  Wenn diese Option ausgewählt ist, müssen Sie als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie einen Datei-Hash, Metadaten oder ein Zertifikat angeben.

  Datei-Hash

  Abhängig von der Version des Sicherheitsprogramms, das auf den Geräten in Ihrem Netzwerk installiert ist, müssen Sie einen Hash-Algorithmus auswählen, den Kaspersky Endpoint Security auf Dateien dieser Kategorie anwenden soll. Informationen über die Hash-Werte, die durch Hash-Funktionen berechnet wurden, sind in der Datenbank des Administrationsservers gespeichert.

  SHA256 ist eine kryptografische Hash-Funktion, deren Algorithmus keine bekannten Schwächen aufweist. Sie gilt derzeit als die sicherste Hash-Funktion. SHA256 wird von Kaspersky Endpoint Security 10 und höher unterstützt. Die MD5-Hash-Funktion wird für ältere Versionen als Kaspersky Endpoint Security 10 unterstützt.

  Wählen Sie eine der Hash-Funktionen aus, die Kaspersky Endpoint Security auf Dateien der folgenden Kategorie anwenden soll:

  - Wenn in Ihrem Netzwerk keine anderen Exemplare von Sicherheitsprogrammen installiert sind als Kaspersky Endpoint Security Version 10 oder höhere Versionen, aktivieren Sie das Kontrollkästchen **SHA256**. Es wird davor gewarnt, eine Kategorie auf Basis des SHA256-Hashs einer ausführbaren Datei für Kaspersky Endpoint Security 10 oder älter zu erstellen. Dies kann dazu führen, dass das Sicherheitsprogramm fehlerhaft funktioniert. In diesem Fall können Sie für Dateien dieser Kategorie die kryptografische MD5-Hash-Funktion verwenden.

  - Wenn in Ihrem Netzwerk ältere Versionen als Kaspersky Endpoint Security 10 installiert sind, aktivieren Sie das Kontrollkästchen **MD5-Hash**. Für Kaspersky Endpoint Security 10 oder höher ist es nicht möglich, eine Kategorie auf Basis des MD5-Hashs einer ausführbaren Datei hinzuzufügen. In diesem Fall können Sie für Dateien dieser Kategorie die kryptografische SHA256-Hash-Funktion verwenden.

  - Wenn es in Ihrem Netzwerk Geräte gibt, die sowohl ältere als auch neuere Versionen als Kaspersky Endpoint Security 10 verwenden, aktivieren Sie beide Kontrollkästchen: **SHA256** und **MD5-Hash**.

  Metadaten

  Wenn diese Option ausgewählt ist, können Sie Metadaten wie Dateiname, Dateiversion und Hersteller angeben. Die Bedingung der Kategorie entspricht nur ausführbaren Dateien mit identischen Metadaten.

  Zertifikat

  Wenn diese Option ausgewählt ist, können Sie Zertifikate aus dem Speicher angeben. Die Bedingung der Kategorie entspricht nur ausführbaren Dateien, die mit dem angegebenen Zertifikat signiert sind.

- **Aus einem MSI-Paket/Archivordner**

  Wenn diese Option ausgewählt ist, können Sie eine MSI-Installationsdatei als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie angeben. Die Metadaten des Installationsprogramms werden an den Administrationsserver gesendet. Programme, deren Installationsprogramm-Metadaten mit dem angegebenen MSI-Installationsprogramm übereinstimmen, werden zur benutzerdefinierten Programmkategorie hinzugefügt.

Schritt 4. Einstellungen

Dieser Schritt ist verfügbar, wenn Sie den folgenden Kategorietyp ausgewählt haben: **Kategorie für ausführbare Dateien von ausgewählten Geräten. Diese ausführbaren Dateien werden automatisch verarbeitet und deren Metriken werden zur Kategorie hinzugefügt**.

Klicken Sie bei diesem Schritt auf **Hinzufügen** und geben Sie die Computer an, deren ausführbare Dateien Kaspersky Security Center in die Programmkategorie aufnehmen soll.

Konfigurieren Sie bei diesem Schritt die folgenden Einstellungen:

- **Algorithmus zur Berechnung der Hash-Funktion**

  Abhängig von der Version des Sicherheitsprogramms, das auf den Geräten in Ihrem Netzwerk installiert ist, müssen Sie einen Hash-Algorithmus auswählen, den Kaspersky Security Center auf Dateien in der Kategorie anwendet. Informationen über die Hash-Werte, die durch Hash-Funktionen berechnet wurden, sind in der Datenbank des Administrationsservers gespeichert.

  SHA256 ist eine kryptografische Hash-Funktion, deren Algorithmus keine bekannten Schwächen aufweist. Sie gilt derzeit als die sicherste Hash-Funktion. Kaspersky Endpoint Security für Linux unterstützt SHA256.

  Wählen Sie einen der Hash-Algorithmen aus, der auf Dateien in der Kategorie angewendet werden soll:

  - Wenn Sie Kaspersky Endpoint Security für Linux auf den geschützten Geräten verwenden, aktivieren Sie das Kontrollkästchen **SHA256 für Dateien in dieser Kategorie berechnen (unterstützt ab Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**.

  - Wenn Sie Kaspersky Endpoint Security für Windows auf den geschützten Geräten verwenden, aktivieren Sie das Kontrollkästchen **MD5 für Dateien in dieser Kategorie berechnen (unterstützt bis Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**.

  Wenn Sie in Ihrem Netzwerk Programme sowohl für Windows als auch für Linux verwenden, aktivieren Sie beide Kontrollkästchen.

- **Daten mit dem Speicher des Administrationsservers synchronisieren**

  Wählen Sie diese Option, wenn Sie möchten, dass der Administrationsserver den angegebenen Ordner (oder die angegebenen Ordner) regelmäßig auf Änderungen überprüft.

  Der Parameter ist standardmäßig deaktiviert.

  Wenn Sie diesen Parameter aktivieren, geben Sie den Zeitabstand (in Stunden) an, in dem der angegebene Ordner (oder die angegebenen Ordner) auf Änderungen überprüft werden soll(en). Der standardmäßige Zeitraum beträgt 24 Stunden.

- **Dateityp**

  In diesem Abschnitt können Sie den Dateityp angeben, den Sie zum Erstellen der Programmkategorie verwenden möchten.

  Alle Dateien. Die Kategorie umfasst alle Dateien. Diese Option ist standardmäßig aktiviert.

  Nur Dateien, die keiner Programmkategorie entsprechen. Die Kategorie umfasst nur Dateien, die nicht zu Programmkategorien gehören.

- **Ordner**

  In diesem Abschnitt können Sie Ordner von ausgewählten Computern angeben, die Dateien enthalten, die Sie zum Erstellen der Programmkategorie verwenden möchten.

  Alle Ordner. Die Kategorie umfasst alle Ordner. Diese Option ist standardmäßig aktiviert.

  Angegebener Ordner. Die Kategorie umfasst nur den angegebenen Ordner. Bei Auswahl dieser Option müssen Sie einen Ordnerpfad angeben.

Schritt 5.

Dieser Schritt ist verfügbar, wenn Sie den folgenden Kategorietyp ausgewählt haben: **Kategorie für ausführbare Dateien aus einem bestimmten Ordner. Ausführbare Dateien von Anwendungen, die sich in dem angegebenen Ordner befinden, werden automatisch verarbeitet und deren Metriken werden zur Kategorie hinzugefügt**.

Geben Sie in diesem Schritt den Ordner an, dessen ausführbare Dateien zum Erstellen der Kategorie verwendet werden sollen.

Konfigurieren Sie die folgenden Einstellungen:

- **Dynamic Link Libraries (.dll) in diese Kategorie aufnehmen**

  Die Programmkategorie enthält Dynamic-Link-Bibliotheken (Dateien im DLL-Format) und die Komponente „Programmkontrolle“ protokolliert die Aktionen solcher im System ausgeführten Bibliotheken. Wenn Dateien im DLL-Format in die Programmkategorie aufgenommen werden, kann sich die Leistungsfähigkeit von Kaspersky Security Center vermindern.

  Dieses Kontrollkästchen ist standardmäßig deaktiviert.

- **Skriptdateien in diese Kategorie aufnehmen**

  Die Programmkategorie enthält Daten zu Skripten, und Skripte werden vom Schutz vor Web-Bedrohungen nicht blockiert. Wenn Skriptdaten in die Programmkategorie aufgenommen werden, kann die Leistungsfähigkeit von Kaspersky Security Center sinken.

  Dieses Kontrollkästchen ist standardmäßig deaktiviert.

- **Algorithmus zur Berechnung der Hash-Funktion**

  Abhängig von der Version des Sicherheitsprogramms, das auf den Geräten in Ihrem Netzwerk installiert ist, müssen Sie einen Hash-Algorithmus auswählen, den Kaspersky Security Center auf Dateien in der Kategorie anwendet. Informationen über die Hash-Werte, die durch Hash-Funktionen berechnet wurden, sind in der Datenbank des Administrationsservers gespeichert.

  SHA256 ist eine kryptografische Hash-Funktion, deren Algorithmus keine bekannten Schwächen aufweist. Sie gilt derzeit als die sicherste Hash-Funktion. Kaspersky Endpoint Security für Linux unterstützt SHA256.

  Wählen Sie einen der Hash-Algorithmen aus, der auf Dateien in der Kategorie angewendet werden soll:

  - Wenn Sie Kaspersky Endpoint Security für Linux auf den geschützten Geräten verwenden, aktivieren Sie das Kontrollkästchen **SHA256 für Dateien in dieser Kategorie berechnen (unterstützt ab Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**.

  - Wenn Sie Kaspersky Endpoint Security für Windows auf den geschützten Geräten verwenden, aktivieren Sie das Kontrollkästchen **MD5 für Dateien in dieser Kategorie berechnen (unterstützt bis Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**.

  Wenn Sie in Ihrem Netzwerk Programme sowohl für Windows als auch für Linux verwenden, aktivieren Sie beide Kontrollkästchen.

- **Untersuchung des Ordners auf Änderungen erzwingen**

  Wenn diese Option aktiviert ist, überprüft das Programm regelmäßig den Ordner zum Hinzufügen von Kategorieinhalten auf Änderungen. Im Eingabefeld neben dem Kontrollkästchen können Sie die Häufigkeit der Überprüfungen (in Stunden) angeben. Standardmäßig beträgt das Zeitintervall zwischen erzwungenen Überprüfungen 24 Stunden.

  Wenn diese Option deaktiviert ist, erzwingt das Programm keine Überprüfungen des Ordners. Der Server versucht, auf Dateien zuzugreifen, wenn sie geändert, hinzugefügt oder gelöscht wurden.

  Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Schritt 6.

Schließen Sie den Assistenten ab. Nach Abschluss des Assistenten wird die neue Programmkategorie erstellt. Sie können Programme aus der Kategorie mithilfe von Regeln der Programmkontrolle kontrollieren.

Golden Image

Sie können die Inventarisierung verwenden, um die Programmkategorie Golden Image hinzuzufügen. Standardmäßig ist die Kategorie leer. Die Kategorie „Goldenes Image“ enthält Programme, die zusammen mit dem Betriebssystem auf dem Gerät bereitgestellt werden. Programme in dieser Kategorie gelten als vertrauenswürdig. Bei Bedarf können Sie der Kategorie Drittanbieter-Programme hinzufügen.

Nach Abschluss der Inventarisierungsaufgabe kann das Programm die Kategorie „Goldenes Image“ wie folgt ändern:

- **Keine Änderungen** – die Kategorie „Goldenes Image“ nach Abschluss der Inventarisierung nicht ändern. Diese Option ist standardmäßig ausgewählt. Diese Option wird verwendet, wenn Sie eine Liste der auf dem Gerät verwendeten Programme von Drittanbietern abrufen möchten, diese jedoch nicht zur Kategorie „Golden Image“ hinzufügen möchten.

- **Aktualisieren oder erstellen (falls nicht vorhanden)** – Programme, die durch die Inventarisierungsaufgabe auf dem Gerät erkannt wurden, zur Kategorie "Goldene Kategorie" hinzufügen. Wenn die Kategorie nicht vorhanden ist, wird sie erstellt. Wenn eine Kategorie existiert, wird die Liste der darin enthaltenen Anwendungen aktualisiert.

- **Entfernen** – die Programmkategorie „Goldenes Image“ leeren. Die Kategorie wird sofort nach dem Start der Aufgabe geleert, ohne dass eine Inventarisierung der Dateien auf dem Gerät durchgeführt wird.

  Dies kann in den folgenden Szenarien nützlich sein:

  - Wenn Sie den Start von Programmen aus der Kategorie „Goldenes Image“ auf dem Gerät verhindern müssen, die Regel der Programmkontrolle jedoch nicht deaktivieren können.

  - Wenn Sie eine neue Richtlinie auf ein Gerät anwenden, das Regeln der Programmkontrolle enthält, die sich von der aktuellen Richtlinie unterscheiden, oder wenn Sie ein Gerät in eine untergeordnete Richtlinie verschieben. In diesem Fall empfehlen wir, die Kategorie „Goldenes Image“ zu leeren, um erlaubte Programme nicht versehentlich zu blockieren.

Konfigurieren der Kategorie „Goldenes Image“ auf Grundlage eines Baseline-Computers

Sie können einen Baseline-Computer verwenden, um eine Kategorie „Goldenes Image“ mit den benötigten Programmen zu erstellen. Anschließend können Sie diese Kategorie verwenden, um Erlaubnisregeln für die Programmkontrolle zu erstellen.

Die Konfiguration der Kategorie „Goldenes Image“ auf Grundlage eines Baseline-Computers umfasst folgende Schritte:

1. **Referenzcomputer konfigurieren**

   Installieren und konfigurieren Sie die gesamte Software, die Sie für den Betrieb der Geräte im Unternehmensnetzwerk benötigen, einschließlich Kaspersky Endpoint Security für Linux und Administrationsagent.

2. **Erstellen einer Aufgabe „Inventarisierung“**

   Erstellen Sie die Aufgabe in der Web Console oder über die Befehlszeile und konfigurieren Sie die folgenden Einstellungen:

   - Aktion für die Programmkategorie „Goldenes Image“: **Aktualisieren oder erstellen (falls nicht vorhanden)**;

     ```
     GoldenImageAction=Create
     ```

   - Der Inventarisierungsbereich ist der Referenzcomputer.

3. **Führen Sie die Inventarisierungsaufgabe aus und warten Sie, bis sie abgeschlossen ist.**

   Die Aufgabe erstellt die Programmkategorie „Goldenes Image“.

4. **Exportieren Sie die Liste der Kategorien in eine Datei.**

   Sie können in der Web Console keine Liste von Kategorien exportieren.

   Führen Sie den Befehl aus:

   ```
   kesl-control [-A] --get-categories --file <path to file> --json
   ```

   Dabei ist `<path to file>` der Pfad zur Konfigurationsdatei, in die Sie die Aufgabeneinstellungen ausgeben möchten.

5. **Passen Sie bei Bedarf Ihre Kategorie „Goldenes Image“ an.**

   Überprüfen Sie die Konfigurationsdatei mit der Liste der Programmkategorien. Nehmen Sie bei Bedarf in der Kategorie „Goldenes Image“ Anpassungen an der Liste der Programme vor.

6. **Importieren Sie die Einstellungen aus der Konfigurationsdatei.**

   Wenn Sie die Konfigurationsdatei mit der Liste der Programmkategorien geändert haben, importieren Sie sie in das Programm:

   ```
   kesl-control [-A] --set-categories --names GoldenImage [<category name 1> <category name 2> ... <name of category N>] --file <path to file>
   ```

   wobei `<category name 1> <category name 2> ... <category name N>` die Namen der Kategorien außer der Kategorie „Goldenes Image“ sind, deren Informationen Sie ändern möchten.

   `<path to file>` ist der Pfad zur Konfigurationsdatei, in die Sie die Aufgabeneinstellungen ausgeben möchten.

Dadurch können Sie die Kategorie „Goldenes Image“ verwenden, um Regeln der Programmkontrolle zu erstellen.

Über die Regeln für die Programmkontrolle

Eine *Regel der Programmkontrolle* ist eine Reihe von Bedingungen, die bestimmen, ob die Programmkontrolle den Start eines Drittanbieter-Programms für eine ausgewählte Gruppe von Benutzern erlaubt oder verbietet.

Die Regeln schränken den Start von Drittanbieter-Programmen anhand der folgenden Kriterien ein:

- **Programmkategorien**. Zugehörigkeit des Programms zu einer Programmkategorie.

  Eine Kategorie kann jeweils nur in einer einzigen Regel verwendet werden.

- **Benutzer und Benutzergruppen**. Mit der Programmkontrolle können Sie den Zugriff auf Drittanbieter-Programme für einzelne Benutzer oder Benutzergruppen einschränken. So können Sie beispielsweise den Zugriff auf Programme zur Remote-Administration für alle Benutzer im Unternehmen mit Ausnahme der Benutzer in der IT-Abteilung einschränken.

Regeln der Programmkontrolle können einen der folgenden *Ausführungsstatus* haben:

- **Aktiviert**. Die Programmkontrolle wendet die Regel an.
- **Deaktiviert**. Die Programmkontrolle wendet die Regel nicht an.
- **Test**. Die Programmkontrolle blockiert die Ausführung von Drittanbieter-Programmen nicht, sendet jedoch Benachrichtigungen über deren Start an den Administrationsserver.

Regeln der Programmkontrolle in der Web Console hinzufügen

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **App-Kontrolle**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **App-Kontrolle AKTIVIERT** befindet.
6. Klicken Sie im Block **Aktion beim Starten von Programmen** auf **Hinzufügen**.

   Das Formular zum Hinzufügen einer Regel der Programmkontrolle wird geöffnet.
7. Legen Sie im Feld **Status** den Status der Regel fest.
8. Wenn Sie die Regel testen möchten, setzen Sie diesen Umschalter auf **Aktiviert** und aktivieren Sie das Kontrollkästchen **Testmodus**.
9. Geben Sie im Feld **Regelname** den Regelnamen ein. Der Relgename muss eindeutig sein.
10. Wählen Sie die Programmkategorie aus, auf die Sie die Regel anwenden möchten. Eine Regel kann nicht gespeichert werden, ohne eine Kategorie anzugeben.
11. Wählen Sie Benutzer oder eine Benutzergruppe und deren Berechtigungen zum Ausführen von Programmen aus.
12. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Regeln der Programmkontrolle über die Befehlszeile hinzufügen

1. Geben Sie die Liste der Regeln der Programmkontrolle in eine Datei aus:

```
kesl-control --get-settings 21 --file <path to file> [--json]
```

2. Öffnen Sie die Konfigurationsdatei und fügen Sie je nach Modus der Programmkontrolle einen Abschnitt für die Regel mit der ID `#` hinzu:

   a. Wenn der Modus `AppControlMode=AllowList`:

   ```
   [AllowListRules.item_#]
   Description=<rule name>
   AppControlRuleStatus=<On|Off|Test>
   Category=<category name>
   [AllowListRules.item_#.ACL.item_#]
   Access=<Allow|Block>
   Principal=<user>
   ```

   ausgewählt ist

   b. Wenn der Modus `AppControlMode=DenyList`:

   ```
   [DenyListRules.item_#]
   Description=<rule name>
   AppControlRuleStatus=<On|Off|Test>
   Category=<category name>
   [DenyListRules.item_#.ACL.item_#]
   Access=<Allow|Block>
   Principal=<user>
   ```

   ausgewählt ist

3. Importieren Sie die Einstellungen aus der Konfigurationsdatei in das Programm:

```
kesl-control --set-settings 21 --file <path to file> [--json]
```

Symbole

Befehlsoptionen

Einstellung	Description
`[AllowListRules.item_#]` `[DenyListRules.item_#]`	Regel der Programmkontrolle mit der ID `#`.
`[AllowListRules.item_#.ACL.item_#]` `[DenyListRules.item_#.ACL.item_#]`	Liste der Benutzer, für die die Regel der Programmkontrolle mit der ID `#` gilt.
`Description`	Regelbeschreibung für die App-Kontrolle
`AppControlRuleStatus`	Der Status der Regel der Programmkontrolle: `On` (Standardwert) – Die Regel ist aktiviert und Kaspersky Endpoint Security wendet diese Regel während der Programmkontrolle an. `Off` – Die Regel wird während der Programmkontrolle 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. Sie können die Kategorie `Golden Image` angeben.
`Access`	Zugriffstyp, der einem Benutzer oder einer Benutzergruppe zugewiesen ist: `Allow` (Standardwert) – Start der Anwendung zulassen. `Block` – Start der Anwendung verbieten.
`Principal`	Benutzer oder Benutzergruppe, für den bzw. die die Regel der Programmkontrolle gilt: `\Everyone` (Standardwert) – Die Regel gilt für alle Benutzer. `<user>` ist der Name des Benutzers, für den die Regel gilt. `@<group name>` ist der Name der Benutzergruppe, für die die Regel gilt.

Testmodus für Regeln der Programmkontrolle

Um sicherzustellen, dass die Programmkontrolle die für den Betrieb erforderlichen Programme nicht blockiert, wird empfohlen, die Regeln der Programmkontrolle zu testen. Im Testmodus blockiert Kaspersky Endpoint Security die Ausführung von Programmen von Drittanbietern und sendet Benachrichtigungen über deren Start an den Administrationsserver.

Standardmäßig erlaubt die Programmkontrolle die Ausführung aller Programme von Drittanbietern mit Ausnahme der Programme, die durch Regeln verboten sind.

Regeln der Programmkontrolle testen

1. **Regeln der Programmkontrolle erstellen**

   Konfigurieren und aktivieren Sie Regeln der Programmkontrolle, die Sie testen möchten. Sie können beispielsweise Regeln erstellen, die die Ausführung aller Programme von Drittanbietern verhindern, mit Ausnahme von Programmen aus den Kategorien „Goldenes Image“ und „Geschäftliche Programme“.

2. **Programmkontrolle im Testmodus aktivieren**

   So aktivieren Sie den Testmodus der Programmkontrolle in der Web Console

   1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
   2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

      Das Eigenschaftenfenster der Richtlinie wird geöffnet.
   3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
   4. Gehen Sie zu **Sicherheitskontrolle** → **App-Kontrolle**.
   5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **App-Kontrolle AKTIVIERT** befindet.
   6. Wählen Sie unter **Aktion beim Starten von Programmen** die Aktion **Informieren** für die Programmkontrolle aus.
   7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

   So aktivieren Sie den Testmodus der Programmkontrolle über die Befehlszeile

   Um den Testmodus für die Programmkontrolle auszuwählen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --set-settings 21 AppControlRulesAction=TestRules
   ```

3. **Testergebnisse überprüfen**

   Überprüfen Sie den Bericht zur Programmkontrolle und die Ereignisse der Komponente, die an Kaspersky Security Center gesendet werden.

So zeigen Sie den Bericht der Programmkontrolle in der Web Console an

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **App-Kontrolle**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **App-Kontrolle AKTIVIERT** befindet.
6. Klicken Sie in der Tabelle mit den Regeln der Programmkontrolle auf die Schaltfläche **Bericht anzeigen**.
7. Das Fenster **Bericht über verbotene Anwendungen im Testmodus** wird geöffnet.
8. Überprüfen Sie die Informationen über den Start verbotener Programme im Testmodus.

So zeigen Sie Ereignisse an, die aus einem Testlauf der Programmkontrolle resultieren

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Überwachung** → **Ereignisauswahlen** aus.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Geben Sie im geöffneten Fenster **Neue Ereignisauswahl** einen Namen für die Auswahl an. Zum Beispiel „Test für Regeln der Programmkontrolle“.
4. Wechseln Sie zum Abschnitt **Ereignisse** und konfigurieren Sie die folgenden Einstellungen:
   - **Anwendungsname** – Kaspersky Endpoint Security für Linux.
   - **Signifikanz** – **Information**.
   - Wählen Sie die Option **Ausgewählte allgemeine Ereignisse einschließen** aus.
   - Aktivieren Sie die Kontrollkästchen neben den Ereignissen **Programmstart im Testmodus verboten** und **Programmstart im Testmodus erlaubt**.
5. Passen Sie bei Bedarf die übrigen Einstellungen an.
6. Speichern Sie die vorgenommenen Änderungen.
7. Klicken Sie auf den Namen der Auswahl, um das Ergebnis der Ereignisauswahl anzuzeigen.

4 Regeln anpassen

Wenn im Testmodus für alle Programme, die der Benutzer zum Arbeiten benötigt, keine Ereignisse über ein Startverbot vorliegen, sind die Regeln korrekt.

Andernfalls bearbeiten Sie die Einstellungen der von Ihnen erstellten Regeln, erstellen Sie zusätzliche Regeln oder löschen Sie die vorhandenen Regeln.

Überwachung der System-Integrität

Die Überwachung der Systemintegrität überwacht Änderungen im Betriebssystem, die auf Sicherheitsverletzungen auf einem Computer hinweisen können. Wenn solche Änderungen erkannt werden, generiert Kaspersky Endpoint Security entsprechende Ereignisse und warnt den Administrator.

Funktionsweise der Überwachung der Systemintegrität

Die Überwachung der Systemintegrität kann in Echtzeit und bei Bedarf erfolgen:

- Die Komponente *Überwachung der Systemintegrität* ermöglicht es Ihnen, Änderungen an den Dateien und Verzeichnissen zu überwachen, die Sie in den Überwachungsbereich aufgenommen haben, und zwar *in Echtzeit*.
- Die Funktion *Prüfung der Systemintegrität* ermöglicht es Ihnen, den aktuellen Status von Objekten zu vergleichen, die in den Überwachungsbereich aufgenommen wurden, mit ihrem aufgezeichneten Status, entweder *nach Zeitplan oder bei Bedarf*.

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.

Besonderheiten und Einschränkungen

- Aufgrund der technischen Beschränkungen des Betriebssystems Linux kann die App nicht erkennen, welcher Benutzer oder Prozess die Änderungen an einer Datei durchgeführt hat.
- Wenn ein Verzeichnis zum Überwachungs- oder Ausschlussbereich hinzugefügt wird, prüft die App nicht, ob das angegebene Verzeichnis existiert.

Überwachung der Systemintegrität in Echtzeit

Die Überwachung der Systemintegrität ermöglicht die Echtzeiterkennung von Änderungen an einem Objekt, das zum Überwachungsbereich gehört.

Funktionsweise der Überwachung der Systemintegrität

1. **Das Programm fängt Ereignisse von Dateioperationen ab**

   Das Programm verwendet einen speziellen Abfangmechanismus, der nur Lesezugriff auf die untersuchte Datei hat.

2. **Das Programm überprüft, ob die Datei geändert wurde.**

Die Überwachung der Systemintegrität verfolgt Änderungen an folgenden Dateieigenschaften:

- Inhalt (`write ()`, `truncate ()` und andere Änderungen)
- Metadaten (Änderung von Zugriffsberechtigungen mit den Befehlen `chmod` oder `chown`)
- Zeitstempel (`utimensat`)
- Erweiterte Attribute (`setxattr`) und sonstige

3. **Abschluss der Untersuchung**

   Das Programm generiert ein Ereignis *System-Integrität verletzt*, wenn die Datei geändert wurde.

Überwachung der Systemintegrität konfigurieren

1. **Überwachung der System-Integrität aktivieren**

   Die Überwachung der System-Integrität ist standardmäßig deaktiviert. Wählen Sie die Geräte aus, auf denen Sie Dateiänderungen in Echtzeit überwachen möchten, und aktivieren Sie auf diesen Geräten die Komponente zur Überwachung der Systemintegrität.

2. **Überwachungsbereich konfigurieren**

   Damit die Komponente funktioniert, muss mindestens ein Überwachungsbereich angegeben werden. Der Überwachungsbereich *Interne Objekte von Kaspersky* (`/opt/kaspersky/kesl/`) ist standardmäßig festgelegt.

   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.

   So konfigurieren Sie einen Überwachungsbereich in der Web Console

   1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
   2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

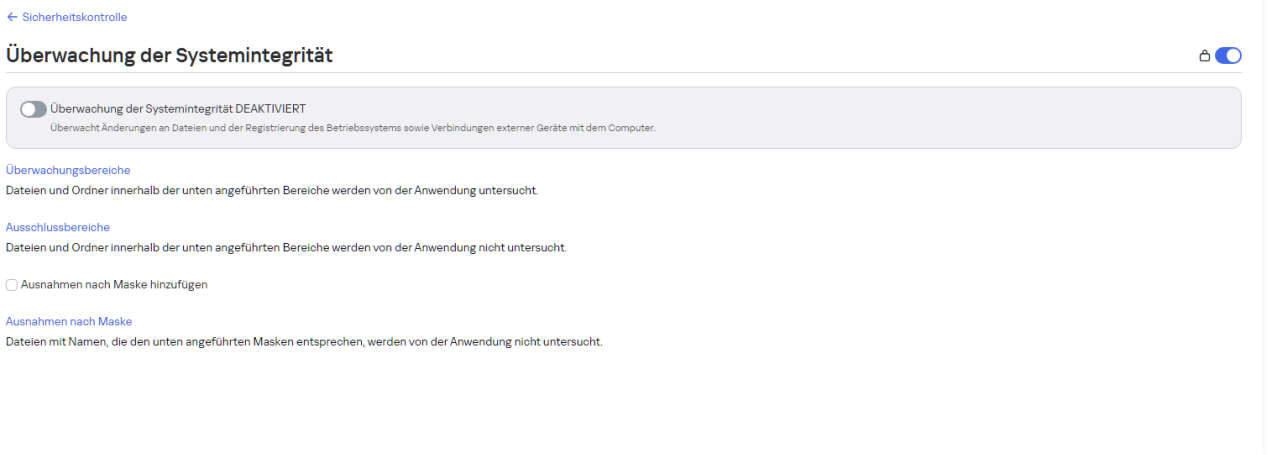
      Das Eigenschaftenfenster der Richtlinie wird geöffnet.
   3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
   4. Gehen Sie zu **Sicherheitskontrolle** → **Überwachung der Systemintegrität**.
   5. Klicken Sie auf den Link **Überwachungsbereiche**.

      Dadurch wird ein Fenster mit einer Tabelle der Untersuchungsbereiche geöffnet.
   6. Klicken Sie auf die Schaltfläche **Hinzufügen**.

      Dadurch wird das Fenster zum Hinzufügen von Untersuchungsbereichen geöffnet
   7. Geben Sie im Feld **Name** den Namen des Überwachungsbereichs an, z. B. *Kritische Objekte*.
   8. Geben Sie im Feld **Pfad** den Pfad zu einer einzelnen Datei oder einem Verzeichnis an (z. B. `/path/to/folder`). Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

9. Geben Sie bei Bedarf Masken für Objektnamen im Format der Befehlsshell an (z. B. `*.txt` oder `file?.*`). Fügen Sie Masken einzeln hinzu.

10. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Überwachung der System-Integrität

So konfigurieren Sie einen Überwachungsbereich über die Befehlszeile

1. Führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 11  ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 11
```

Symbole

Befehlsoptionen

Parameter	Description
`UseScanArea=Yes`	Aktivieren eines Überwachungsbereichs mit einer `#`-ID. Sie können die Untersuchung eines Überwachungsbereichs vorübergehend deaktivieren, anstatt den Bereich zu löschen. Legen Sie dazu `ScanScope.item_#.UseScanArea=No` fest.
`AreaDesc`	Beschreibung des Überwachungsbereichs mit zusätzlichen Informationen über den Überwachungsbereich.
`AreaMask.item_#`	Einschränkung des Überwachungsbereichs. Im Überwachungsbereich untersucht die Anwendung nur Objekte, die mit Masken im Shell-Format angegeben wurden. Beispiel: `ScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Pfad zum Verzeichnis, das überwacht werden soll. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

Beispiel

Ein Überwachungsbereich, der nur das Verzeichnis `/etc` umfasst:

```
kesl-control --set-settings 11 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/etc
```

3 Ausschlussbereich anpassen

Eine Ausnahme hat eine höhere Priorität als ein Überwachungsbereich. Ein ausgenommenes Objekt wird nicht untersucht, selbst wenn es sich in einem 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.

So konfigurieren Sie einen Ausnahmebereich in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **Überwachung der Systemintegrität**.

Sie können Ausnahmen nach Pfad oder Dateinamenmaske angeben. Das Programm kann ein gesamtes Verzeichnis (oder eine einzelne Datei) von der Untersuchung ausschließen oder Dateien mit einer passenden Namensmaske in Überwachungsbereichen ausschließen.

So fügen Sie Ausnahmen nach Pfad hinzu:

1. Klicken Sie auf den Link **Ausschlussbereiche**.

   Dadurch wird ein Fenster mit einer Tabelle der Ausnahmebereiche geöffnet.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster zum Hinzufügen von Ausnahmebereichen wird geöffnet.
3. Geben Sie im Feld **Name** den Namen des Ausnahmebereichs an, z. B. *Systemdateien*.
4. Geben Sie im Feld **Pfad** den Pfad zu einer einzelnen Datei oder einem Verzeichnis an (z. B. `/path/to/folder`). Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.
5. Geben Sie Masken für Objektnamen im Format der Befehlsshell an (z. B. `*.txt` oder `file?.*`). Fügen Sie Masken einzeln hinzu.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So fügen Sie Ausnahmen nach Dateinamenmaske hinzu:

1. Aktivieren Sie das Kontrollkästchen **Ausnahmen nach Maske hinzufügen**.
2. Klicken Sie auf den Link **Ausnahmen nach Maske**.

   Dadurch wird eine Tabelle mit Ausnahmebereichen nach Maske geöffnet.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Dadurch wird das Fenster zum Hinzufügen von Ausnahmebereichen nach Maske geöffnet.
4. Geben Sie die Dateinamenmaske im Format der Befehlsshell an (z. B. `*.txt` oder `file?.*`). Fügen Sie Masken einzeln hinzu.
5. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie einen Ausnahmebereich über die Befehlszeile

1. Führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 11  ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 11
```

Symbole

Befehlsoptionen

Parameter	Description
`UseScanArea=Yes`	Nimmt den angegebenen Bereich mit der ID `#` von der Überwachung aus. Sie können einen Ausnahmebereich vorübergehend deaktivieren, anstatt den Bereich zu löschen. Legen Sie dazu `ExcludedFromScanScope.item_#.UseScanArea=No` fest.
`AreaDesc`	Beschreibung des Ausschlussbereichs von der Überwachung mit zusätzlichen Informationen über den Ausschlussbereich von der Überwachung.
`AreaMask.item_#`	Einschränkung des Ausnahmebereichs. Im Ausnahmebereich nimmt die Anwendung nur die Objekte von Untersuchungen aus, die mithilfe von Masken im Shell-Format angegeben wurden. Beispiel: `ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Der Pfad zum Verzeichnis, das von der Untersuchung ausgenommen werden soll. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

Beispiel

Ein Ausnahmebereich, der nur das Verzeichnis `/tmp` enthält:

```
kesl-control --set-settings 11 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

Prüfung der Systemintegrität

Während der Ausführung der Aufgabe *Prüfung der Systemintegrität* vergleicht das Programm den aktuellen Zustand jedes Objekts mit seinem ursprünglichen Zustand, der Baseline. Die Baseline enthält Pfade zu überwachten Objekten und deren Metadaten. Dadurch können Änderungen an Dateien und Verzeichnissen verfolgt werden, die in den Überwachungsbereich eingeschlossen sind.

Eine Baseline kann auch personenbezogene Daten enthalten.

Im Gegensatz zur Komponente Überwachung der Systemintegrität hilft die Aufgabe *Prüfung der Systemintegrität* dabei, die Anzahl der Ereignisse zu begrenzen, und ermöglicht es Ihnen, einen zusammenfassenden Bericht über Änderungen im Betriebssystem zu erstellen.

Funktionsweise der Prüfung der Systemintegrität

1. **Das Programm erstellt eine Momentaufnahme des Systems**

   Die Baseline des Systems wird bei der ersten Ausführung der Aufgabe erstellt. Wenn Sie mehrere Aufgaben zur Prüfung der Systemintegrität erstellt haben, wird für jede Aufgabe eine separate Baseline erstellt. Für Linux-Geräte wird eine Baseline neu erstellt, wenn sich die Aufgabeneinstellungen ändern, z. B. wenn ein neuer Überwachungsbereich hinzugefügt wird, sowie wenn die Aufgabe mit aktivierter Einstellung **Baseline bei jedem Aufgabenstart neu erstellen** gestartet wird.

   Der Speicher für Baselines befindet sich unter `/var/opt/kaspersky/kesl/private/fim.db`. Für den Zugriff auf die Datenbank mit Baselines sind Root-Rechte erforderlich. Die Baseline wird zusammen mit der zugehörigen Aufgabe zur Prüfung der Systemintegrität gelöscht.

2. **Das Programm sucht nach Änderungen des Systemzustands**

   Das Programm verwendet die folgenden Kriterien, um Informationen über Objekte zu vergleichen, die in den Überwachungsbereich eingeschlossen sind:

   - SHA256-Hash der Datei (für eine vollständige Prüfung)
   - Änderungszeit der Datei
   - Dateigröße

3. **Abschluss der Untersuchung**

   Wenn der aktuelle Zustand des Systems von der Baseline abweicht, generiert Kaspersky Endpoint Security ein Ereignis zur Verletzung der Systemintegrität: *System-Integrität verletzt*.

Konfigurieren und Ausführen der Aufgabe zur Prüfung der Systemintegrität

1. **Aufgabe zur Prüfung der Systemintegrität erstellen**

   So erstellen Sie die Aufgabe zur Prüfung der Systemintegrität in der Web Console

   1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

      Die Aufgabenliste wird geöffnet.

   2. Klicken Sie auf **Hinzufügen**.

      Der Assistent für neue Aufgaben wird gestartet.

   3. Passen Sie die Einstellungen der Aufgabe an:

      a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Linux 12.5**.

      b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Prüfung der Systemintegrität**.

      c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *Wöchentliche Prüfung der Systemintegrität*.

      d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

   4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe.

   5. Schließen Sie den Assistenten ab.

   So erstellen Sie die Aufgabe zur Prüfung der Systemintegrität über die Befehlszeile

   Um eine Aufgabe zu erstellen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --create-task <task name> --type ODFIM
   ```

   wobei `<task name>` der Name der neuen Aufgabe ist.

   Dieser Befehl gibt die ID der erstellten Aufgabe zurück.

   Beispiel für das Ergebnis der Befehlsausführung:

   Aufgabe erstellt (Aufgaben-ID: 115)

2. **Bearbeiten Sie bei Bedarf die Aufgabeneinstellungen**

   So konfigurieren Sie die Aufgabe zur Prüfung der Systemintegrität in der Web Console

   1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

      Die Aufgabenliste wird geöffnet.

   2. Klicken Sie auf die neu erstellte Aufgabe zur Prüfung der Systemintegrität.

      Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wählen Sie den Untersuchungstyp aus:

   - **Vollständige Untersuchung**. Das Programm vergleicht den SHA256-Hash der Datei in ihrem aktuellen Zustand mit dem Hash aus der Momentaufnahme des Systems.

   - **Schnelle Untersuchung**. Das Programm vergleicht nur die Dateigrößen. Wenn sich die Dateigröße nicht geändert hat, wird der Änderungszeitpunkt nicht als kritischer Parameter betrachtet.

5. Aktivieren Sie im Abschnitt **Einstellungen für die Prüfung der Systemintegrität** die Kontrollkästchen:

   - **Baseline bei jedem Aufgabenstart neu erstellen**. Wenn dieses Kontrollkästchen aktiviert ist, erstellt das Programm die Baseline bei jedem Start der Aufgabe neu.

   - **Verzeichnisse in Überwachungsbereichen überwachen**. Wenn dieses Kontrollkästchen aktiviert ist, überprüft das Programm die vom Benutzer angegebenen Verzeichnisse. Wenn das Kontrollkästchen deaktiviert ist, untersucht die App nur den standardmäßigen Untersuchungsbereich – *Interne Kaspersky-Objekte* (`/opt/kaspersky/kesl/`).

   - **Bei jedem Aufgabenstart überprüfen, wann zuletzt auf eine Datei zugegriffen wurde**. Wenn dieses Kontrollkästchen aktiviert ist, überprüft das Programm bei jeder Ausführung der Aufgabe den Zeitpunkt des letzten Zugriffs auf die Datei (den Parameter `noatime`).

6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Aufgabe zur Prüfung der Systemintegrität über die Befehlszeile

Führen Sie den Befehl aus:

```
kesl-control --set-settings <task ID|name> RebuildBaseline=<Yes|No> [CheckFileHash=<Yes|No>]
[TrackDirectoryChanges=<Yes|No>] [TrackLastAccessTime=<Yes|No>] [UseExcludeMasks=<Yes|No>]
[ExcludeMasks.item_#=<object mask>]
```

Symbole

Einstellungen der Aufgabe *Prüfung der Systemintegrität*

Parameter	Description
`RebuildBaseline`	Baseline bei jedem Start der Aufgabe neu erstellen.
`CheckFileHash`	Untersuchung des SHA256-Hashwerts der Datei. 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`	Untersuchung der vom Benutzer angegebenen Verzeichnisse. Wenn die Einstellung deaktiviert ist, untersucht das Programm nur den Standardbereich (`/opt/kaspersky/kesl/`).
`TrackLastAccessTime`	Überprüfung des Zeitpunkts des letzten Zugriffs auf die Datei (Option `noatime`).
`UseExcludeMasks`	Ausnahmen von der Überwachung. Den Aufgabeneinstellungen wird ein neuer Abschnitt vom Typ `[ExcludeMasks.item_#]` hinzugefügt. Das Programm wird die in diesem Abschnitt angegebenen Objekte nicht untersuchen. Diese Einstellung funktioniert nur, wenn die Einstellung `ExcludeMasks.item_#` angegeben ist.
`ExcludeMasks.item_#=<object mask>`	Ausschließen von Objekten aus dem Überwachungsbereich. Mit dieser Einstellung können Sie eine einzelne Datei anhand des Namens oder mehrere Dateien anhand von Masken im Format der Befehlsschnittstelle aus dem angegebenen Untersuchungsbereich ausschließen. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske. Diese Einstellung kann nur verwaltet werden, wenn der Parameter `UseExcludeMasks` aktiviert ist. Sie können mehrere Masken angeben. Jede Maske muss in einer neuen Zeile mit einem neuen Index angegeben werden. Beispiel: `ExcludeMasks.item_0000=<eicar1.*>`

3 Überwachungsbereich konfigurieren

Damit die Aufgabe gestartet werden kann, muss mindestens ein Überwachungsbereich festgelegt sein. Der Überwachungsbereich *Interne Objekte von Kaspersky* (`/opt/kaspersky/kesl/`) ist standardmäßig festgelegt.

Die Aufgabe wird nur ausgeführt, wenn die Baseline Informationen über Objekte enthält, die zum Überwachungsbereich der Aufgabe gehören.

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.

So konfigurieren Sie einen Überwachungsbereich in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die neu erstellte Aufgabe zur Prüfung der Systemintegrität.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Stellen Sie sicher, dass das Kontrollkästchen **Verzeichnisse in Überwachungsbereichen überwachen** aktiviert ist.

5. Klicken Sie im Block **Überwachungs- und Ausschlussbereiche** auf den Link **Überwachungsbereiche**.

   Dadurch wird ein Fenster mit einer Tabelle der Untersuchungsbereiche geöffnet.

6. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Dadurch wird das Fenster zum Hinzufügen von Untersuchungsbereichen geöffnet

7. Geben Sie im Feld **Name** einen Namen für den Überwachungsbereich ein, z. B. *Dateien auf dem Desktop*.

8. Geben Sie im Feld **Pfad** den Pfad zu einer einzelnen Datei oder einem Verzeichnis an (z. B. `/path/to/folder`). Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

9. Geben Sie bei Bedarf Masken für Objektnamen im Format der Befehlsshell an (z. B. `*.txt`, `file?.*`). Fügen Sie Masken einzeln hinzu.

10. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie einen Überwachungsbereich über die Befehlszeile

1. Führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings <task ID|name> TrackDirectoryChanges=Yes ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. Um die aktuellen Einstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings <task ID|name>
```

Symbole

Einstellungen der Aufgabe *Prüfung der Systemintegrität*

Parameter	Description
`UseScanArea=Yes`	Aktivieren eines Überwachungsbereichs mit einer `#`-ID. Sie können die Untersuchung eines Überwachungsbereichs vorübergehend deaktivieren, anstatt den Bereich zu löschen. Legen Sie dazu `ScanScope.item_#.UseScanArea=No` fest.
`AreaDesc`	Beschreibung des Überwachungsbereichs mit zusätzlichen Informationen über den Überwachungsbereich.
`AreaMask.item_#`	Einschränkung des Überwachungsbereichs. Im Überwachungsbereich untersucht die Anwendung nur Objekte, die mit Masken im Shell-Format angegeben wurden. Sie können mehrere Elemente vom Typ `ScanScope.item_#.AreaMask.item_#` in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge. Beispiel: `ScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Pfad zum Verzeichnis, das überwacht werden soll. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

Beispiel

Ein Überwachungsbereich, der nur das Verzeichnis `/etc` umfasst:

```
kesl-control --set-settings 115 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/etc
```

4 Ausschlussbereich anpassen

Eine Ausnahme hat eine höhere Priorität als ein Überwachungsbereich. Ein ausgenommenes Objekt wird nicht untersucht, selbst wenn es sich in einem 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.

So konfigurieren Sie einen Ausnahmebereich in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.
2. Die Aufgabenliste wird geöffnet.
3. Klicken Sie auf die neu erstellte Aufgabe zur Prüfung der Systemintegrität.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.
4. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

Sie können Ausnahmen nach Pfad oder Dateinamenmaske angeben. Das Programm kann ein gesamtes Verzeichnis (oder eine einzelne Datei) von der Untersuchung ausschließen oder Dateien mit einer passenden Namensmaske in Überwachungsbereichen ausschließen.

So fügen Sie Ausnahmen nach Pfad hinzu:

1. Klicken Sie im Block **Überwachungs- und Ausschlussbereiche** auf den Link **Ausschlussbereiche**.

   Dadurch wird ein Fenster mit einer Tabelle der Ausnahmebereiche geöffnet.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster zum Hinzufügen von Ausnahmebereichen wird geöffnet.
3. Geben Sie im Feld **Name** den Namen des Ausnahmebereichs an, z. B. *Systemdateien*.

4. Geben Sie im Feld **Pfad** den Pfad zu einer einzelnen Datei oder einem Verzeichnis an (z. B. `/path/to/folder`). Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

5. Geben Sie Masken für Objektnamen im Format der Befehlsshell an (z. B. `*.txt` oder `file?.*`). Fügen Sie Masken einzeln hinzu.

6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So fügen Sie Ausnahmen nach Dateinamenmaske hinzu:

1. Klicken Sie im Block **Überwachungs- und Ausschlussbereiche** auf den Link **Ausnahmen nach Maske**.

   Dadurch wird eine Tabelle mit Ausnahmebereichen nach Maske geöffnet.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Dadurch wird das Fenster zum Hinzufügen von Ausnahmebereichen nach Maske geöffnet.

3. Geben Sie die Dateinamenmaske im Format der Befehlsshell an (z. B. `*.txt` oder `file?.*`). Fügen Sie Masken einzeln hinzu.

4. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie einen Ausnahmebereich über die Befehlszeile

1. Führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings <task ID|name>      ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. Um die aktuellen Einstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings <task ID|name>
```

Symbole

Einstellungen der Aufgabe *Prüfung der Systemintegrität*

Parameter	Description
`UseScanArea=Yes`	Nimmt den angegebenen Bereich mit der ID `#` von der Überwachung aus. Sie können einen Ausnahmebereich vorübergehend deaktivieren, anstatt den Bereich zu löschen. Legen Sie dazu `ExcludedFromScanScope.item_#.UseScanArea=No` fest.
`AreaDesc`	Beschreibung des Ausschlussbereichs von der Überwachung mit zusätzlichen Informationen über den Ausschlussbereich von der Überwachung.
`AreaMask.item_#`	Einschränkung des Ausnahmebereichs. Im Ausnahmebereich nimmt die Anwendung nur die Objekte von Untersuchungen aus, die mithilfe von Masken im Shell-Format angegeben wurden. Sie können mehrere Elemente vom Typ `ExcludedFromScanScope.item_#.AreaMask.item_#` in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge. Beispiel: `ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Der Pfad zum Verzeichnis, das von der Untersuchung ausgenommen werden soll. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

Beispiel

Ein Ausnahmebereich, der nur das Verzeichnis `/tmp` enthält:

```
kesl-control --set-settings 115 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

5. **Aufgabe ausführen**

So führen Sie die Aufgabe zur Prüfung der Systemintegrität in der Web Console aus

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Aktivieren Sie das Kontrollkästchen neben der erstellten Aufgabe.

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

So führen Sie die Aufgabe zur Prüfung der Systemintegrität über die Befehlszeile aus

Um die Aufgabe auszuführen, führen Sie den folgenden Befehl aus:

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

wobei:

- `<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `[-W]` – Gibt die aktuellen Ereignisse mit Bezug auf diese Aufgabe aus.
- `[--progress]` – Aktiviert das Anzeigen des Ausführungsfortschritts der Aufgabe.

Vertrauenswürdige Zone

Die *vertrauenswürdige Zone* ist eine Liste mit Objekten und Programmen, die nicht von Kaspersky Endpoint Security untersucht werden. Diese Liste wird vom Systemadministrator erstellt.

Die vertrauenswürdige Zone wird manuell vom Systemadministrator angelegt. Berücksichtigt werden dabei die Besonderheiten von Objekten, die für die Arbeit erforderlich sind, sowie die Programme, die auf dem Computer installiert sind. Die Aufnahme von Objekten und Programmen in die vertrauenswürdige Zone kann beispielsweise erforderlich sein, wenn Kaspersky Endpoint Security den Zugriff auf ein bestimmtes Objekt oder Programm blockiert, Sie aber sicher sind, dass dieses Objekt oder Programm unschädlich ist.

Einstellungen	Description
Webadressen	Webadressen, die die Komponente Schutz vor Web-Bedrohungen als vertrauenswürdig einstuft. Der von diesen Adressen ein- und ausgehende Datenverkehr wird von der Komponente nicht auf Bedrohungen untersucht. Die Liste vertrauenswürdiger Adressen kann beispielsweise verwendet werden, wenn die Komponente den Download einer Datei von einer bekannten Website beeinträchtigt. Weitere Informationen finden Sie im Artikel So fügen Sie vertrauenswürdige Webadressen hinzu
IP-Adressen	IP-Adressen von vertrauenswürdigen Geräten. Die Komponente Schutz vor Netzwerkbedrohungen blockiert keine Netzwerkaktivität von diesen Adressen. Für Netzwerkangriffe von den IP-Adressen, die zur Ausnahmeliste gehören, nimmt das Programm keine Informationen in den Bericht auf. Weitere Informationen finden Sie im Artikel So fügen Sie eine vertrauenswürdige IP-Adresse eines Computers hinzu
Netzwerkports	Liste der Netzwerkports, die die Komponente Schutz vor Netzwerkbedrohungen von der Untersuchung ausschließt. Weitere Informationen finden Sie im Artikel So wählen Sie überwachte Netzwerkports aus
Stammzertifikate	Stammzertifikate, die Kaspersky Endpoint Security als vertrauenswürdig einstuft. Die Liste vertrauenswürdiger Stammzertifikate wird verwendet, wenn die Komponenten Schutz vor Web-Bedrohungen, Schutz vor E-Mail-Bedrohungen und Web-Kontrolle verschlüsselte Verbindungen (HTTPS-Verbindungen) untersuchen. Weitere Informationen finden Sie im Artikel So fügen Sie ein Zertifikat zur Liste der vertrauenswürdigen Stammzertifikate hinzu
Domänen	Liste der vertrauenswürdigen Domänen. Die Komponenten Schutz vor Web-Bedrohungen und Web-Kontrolle kontrollieren keine verschlüsselten Verbindungen mit diesen Domänen. Weitere Informationen finden Sie im Artikel So fügen Sie eine vertrauenswürdige Domäne hinzu
Mount-Points	Liste der vertrauenswürdigen Mount-Points. Die Komponenten Schutz vor bedrohlichen Dateien, Schutz vor Verschlüsselung und Untersuchung von Containern schließen die angegebenen Mount-Punkte von der Untersuchung aus. Die Mountpunkte müssen genau so angegeben werden, wie sie in der Ausgabe des Befehls `mount` angezeigt werden. Weitere Informationen finden Sie im Artikel „So schließen Sie Mount-Punkte aus"
Programme	Programme, für die Kaspersky Endpoint Security die Datei- und Netzwerkaktivität sowie den Zugriff auf die Systemregistrierung nicht kontrolliert. Schutzkomponenten wie Schutz vor bedrohlichen Dateien oder Verhaltensanalyse kontrollieren die Aktivität der angegebenen Programme nicht. Weitere Informationen finden Sie im Artikel So fügen Sie vertrauenswürdige Programme hinzu
Ausnahmen für die Schadsoftware-Untersuchung	Dateien oder Ordner sowie Objekttypen (gemäß der Viren-Enzyklopädie), die durch alle oder bestimmte Programmkomponenten von der Untersuchung ausgeschlossen sind. Weitere Informationen finden Sie im Artikel So fügen Sie Schutzausnahmen hinzu
Geräte	Geräte, auf die die Komponente Gerätekontrolle ausgewählten Benutzern oder Gruppen immer vollständigen Zugriff gewährt. Weitere Informationen finden Sie im Artikel So fügen Sie vertrauenswürdige Geräte hinzu

So fügen Sie Schutzausnahmen hinzu

Ein *Ausschluss aus dem Schutz* ist eine Reihe von Bedingungen, die erfüllt sein müssen, damit die Anwendung Kaspersky Endpoint Security Objekte nicht auf Viren und andere Schadsoftware überprüft.

Sie können Schutzausnahmen auf folgende Arten hinzufügen:

- **Ausnahmen nach Pfad**. Pfad zu einer Datei oder einem Verzeichnis oder eine Pfadmaske. Der Pfad zu einem Verzeichnis muss mit einem Schrägstrich `/` enden.

  Um Pfade in Containern oder Images anzugeben, verwenden Sie Tags.

  So verwenden Sie Tags

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Wobei gilt:

`<id>` ist die Container-ID.

`<name>` ist ein Containername

`<path to local directory>` ist der Pfad zum lokalen Verzeichnis.

Sie können auch eindeutige Kombinationen von Tags verwenden: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` und `[image-name:<name>]/path to local directory>`.

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>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

- **Ausnahmen nach Maske**. Maske für den Objektnamen. Die Anwendung untersucht keine Dateien, deren Namen die angegebenen Masken enthalten.
- **Ausnahmen nach Name der Bedrohung** Name des Objekttyps gemäß der Klassifikation der Kaspersky-Enzyklopädie (z. B. `Email-Worm`, `Rootkit` oder `RemoteAdmin`). Sie können den Namen einer Bedrohung mithilfe einer Maske angeben.
- **Ausnahmen nach Prozess** Pfad zu einem Prozess oder eine Pfadmaske für einen Prozess. Der Pfad zu einem Verzeichnis muss mit einem Schrägstrich `/` enden.

Kaspersky Endpoint Security ermöglicht außerdem das Ausschließen von Dateien bestimmter Formate: Archive, E-Mail-Datenbanken, Textdateien, Datenbank-Protokolldateien.

So geben Sie Masken für Ausnahmen nach Pfad an

Das Programm unterstützt Masken zum Festlegen von Untersuchungsausnahmen anhand des Pfads zu einer Datei, einem Verzeichnis oder einem Prozess:

- Das Zeichen `*` (Sternchen) steht als Platzhalter für eine beliebige Zeichenfolge, mit Ausnahme der Zeichen `\` und `/` (Trennzeichen für Datei- und Verzeichnisnamen in Pfaden zu Dateien und Verzeichnissen). Beispiel: Die Maske `/dir/*/*.txt` umfasst alle Pfade zu Dateien mit der Erweiterung TXT, die sich in Verzeichnissen innerhalb des Verzeichnisses `dir` befinden, jedoch nicht in deren Unterverzeichnissen.

- Die Zeichen `**` stehen in Datei- oder Verzeichnisnamen als Platzhalter für eine beliebige Zeichenfolge (auch eine leere Zeichenfolge), einschließlich der Zeichen `\` und `/` (Trennzeichen für Datei- und Verzeichnisnamen in Pfaden zu Dateien und Verzeichnissen). Beispiel: Die Maske `/dir/**/*.txt` umfasst alle Pfade zu Dateien mit der Erweiterung TXT, die sich in Verzeichnissen innerhalb des Verzeichnisses `dir` befinden, jedoch nicht im Verzeichnis `dir` selbst.

- Das Zeichen `?` (Fragezeichen) steht als Platzhalter für ein beliebiges einzelnes Zeichen, mit Ausnahme der Zeichen `\` und `/` (Trennzeichen für Datei- und Verzeichnisnamen in Pfaden zu Dateien und Verzeichnissen). Beispiel: Die Maske `/dir/???.txt` umfasst die Pfade aller Dateien im Verzeichnis `dir`, die die Erweiterung TXT haben und deren Name aus drei Zeichen besteht.

Kaspersky Endpoint Security kann mithilfe von Masken angegebene Ausnahmen je nach ausgewähltem Mechanismus zum Abfangen von Systemereignissen (aktualisierbares Kernel-Modul oder fanotify-Technologie) unterschiedlich verarbeiten. Die folgende Tabelle zeigt anhand eines Beispiels, wie mithilfe von Masken angegebene Ausnahmen bei Verwendung der fanotify-Technologie und des aktualisierbaren Kernel-Moduls verarbeitet werden. Einzelheiten zur Verarbeitung von Ausnahmen beim aktualisierbaren Kernel-Modul finden Sie in der Tabelle *Unterschiede bei mithilfe von Masken angegebenen Ausnahmen für das aktualisierbare Kernel-Modul*.

Beispiel für mithilfe von Masken angegebene Ausnahmen für die fanotify-Technologie und das aktualisierbare Kernel-Modul

Struktur	Ausnahme	Ergebnis
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home Diese Pfadmaske schließt alle Objekte im Verzeichnis /home und in dessen Unterverzeichnissen aus. Die Richtlinie kann auf verschiedene Geräte angewendet werden, wobei eicar auf einem Gerät als Verzeichnisname und auf einem anderen als Dateiname verwendet wird. In diesem Fall werden sowohl die Datei mit dem Namen eicar als auch das Verzeichnis von der Untersuchung ausgeschlossen.	/home/ ├── eicar – **Ausgeschlossen** ├── eicar.txt – **Ausgeschlossen** ├── eicar.file – **Ausgeschlossen** └── test1/ – **Ausgeschlossen** │ ├── eicar – **Ausgeschlossen** │ ├── eicar.txt – **Ausgeschlossen** │ ├── eicar.file – **Ausgeschlossen** │ └── level1/ – **Ausgeschlossen** │ │ ├── eicar – **Ausgeschlossen** │ │ ├── eicar.txt – **Ausgeschlossen** │ │ ├── eicar.file – **Ausgeschlossen** │ │ └── level2/ – **Ausgeschlossen** /home2/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ └── eicar.file – Untersucht

Struktur	Ausnahme	Ergebnis
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/ Diese Pfadmaske schließt alle Objekte im Verzeichnis /home und in dessen Unterverzeichnissen aus.	

Struktur	Ausnahme	Ergebnis
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/* Diese Pfadmaske schließt alle Objekte im Verzeichnis /home und in dessen Unterverzeichnissen aus.	

Struktur	Ausnahme	Ergebnis
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/*.txt Diese Pfadmaske schließt Dateien mit der Erweiterung TXT im Verzeichnis /home von der Untersuchung aus.	/home/ ├── eicar – Untersucht ├── eicar.txt – **Ausgeschlossen** ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ ├── eicar.file – Untersucht │ │ └── level2/ – Untersucht /home2/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ └── eicar.file – Untersucht

Struktur	Ausnahme	Ergebnis
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/*.* Diese Pfadmaske schließt Dateien beliebigen Formats im Verzeichnis /home von der Untersuchung aus.	/home/ ├── eicar – Untersucht ├── eicar.txt – **Ausgeschlossen** ├── eicar.file – **Ausgeschlossen** └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ ├── eicar.file – Untersucht │ │ └── level2/ – Untersucht /home2/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ └── eicar.file – Untersucht

Struktur	Ausnahme	Ergebnis
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/**.txt Dieses Pfadmuster schließt Dateien mit der Erweiterung TXT im Verzeichnis /home und seinen Unterverzeichnissen von der Untersuchung aus.	/home/ ├── eicar – Untersucht ├── eicar.txt – **Ausgeschlossen** ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – **Ausgeschlossen** │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – **Ausgeschlossen** │ │ ├── eicar.file – Untersucht │ │ └── level2/ – Untersucht /home2/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ └── eicar.file – Untersucht

Struktur	Ausnahme	Ergebnis
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/**.* Dieses Pfadmuster schließt Dateien aller Formate im Verzeichnis /home und seinen Unterverzeichnissen von der Untersuchung aus.	/home/ ├── eicar – Untersucht ├── eicar.txt – **Ausgeschlossen** ├── eicar.file – **Ausgeschlossen** └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – **Ausgeschlossen** │ ├── eicar.file – **Ausgeschlossen** │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – **Ausgeschlossen** │ │ ├── eicar.file – **Ausgeschlossen** │ │ └── level2/ – Untersucht /home2/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ └── eicar.file – Untersucht

Struktur	Ausnahme	Ergebnis
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/*/*.txt Diese Pfadmaske schließt Dateien mit der Erweiterung .TXT im Verzeichnis der ersten Ebene relativ zum Verzeichnis /home aus.	/home/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – **Ausgeschlossen** │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ ├── eicar.file – Untersucht │ │ └── level2/ – Untersucht /home2/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ └── eicar.file – Untersucht

Struktur	Ausnahme	Ergebnis
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/*/*.* Diese Pfadmaske schließt Dateien aller Formate im Verzeichnis der ersten Ebene relativ zum Verzeichnis /home aus.	/home/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – **Ausgeschlossen** │ ├── eicar.file – **Ausgeschlossen** │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ ├── eicar.file – Untersucht │ │ └── level2/ – Untersucht /home2/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ └── eicar.file – Untersucht

Struktur	Ausnahme	Ergebnis
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/**/*.txt Diese Pfadmaske schließt Dateien mit der Erweiterung TXT im Verzeichnis /home aus; die Anwendung untersucht TXT-Dateien direkt im Verzeichnis /home.	/home/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – **Ausgeschlossen** │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – **Ausgeschlossen** │ │ ├── eicar.file – Untersucht │ │ └── level2/ – Untersucht /home2/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ └── eicar.file – Untersucht

Struktur	Ausnahme	Ergebnis
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/*/* oder /home/**/* Diese Pfadmaske schließt Dateien aller Formate, einschließlich Dateien ohne Erweiterung, in Unterverzeichnissen von /home aus; das Programm untersucht Dateien direkt im Verzeichnis /home.	/home/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ │ ├── eicar – **Ausgeschlossen** │ ├── eicar.txt – **Ausgeschlossen** │ ├── eicar.file – **Ausgeschlossen** │ └── level1/ – Untersucht │ │ ├── eicar – **Ausgeschlossen** │ │ ├── eicar.txt – **Ausgeschlossen** │ │ ├── eicar.file – **Ausgeschlossen** │ │ └── level2/ – Untersucht /home2/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ └── eicar.file – Untersucht

Struktur	Ausnahme	Ergebnis
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/eicar Diese Pfadmaske schließt Dateien ohne Erweiterung mit dem Namen eicar im Verzeichnis /home aus.	/home/ ├── eicar – **Ausgeschlossen** ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ ├── eicar.file – Untersucht │ │ └── level2/ – Untersucht /home2/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ └── eicar.file – Untersucht

Struktur	Ausnahme	Ergebnis
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/*/eicar Diese Pfadmaske schließt Dateien ohne Erweiterung mit dem Namen eicar im Verzeichnis der ersten Ebene unterhalb des Verzeichnisses /home aus.	/home/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – **Ausgeschlossen** │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ ├── eicar.file – Untersucht │ │ └── level2/ – Untersucht /home2/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ └── eicar.file – Untersucht

Struktur	Ausnahme	Ergebnis
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/**/eicar Diese Pfadmaske schließt Dateien ohne Dateinamenerweiterung mit dem Namen eicar in Unterverzeichnissen von /home aus; die Anwendung untersucht Dateien direkt im Verzeichnis /home.	/home/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – **Ausgeschlossen** │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – **Ausgeschlossen** │ │ ├── eicar.txt – Untersucht │ │ ├── eicar.file – Untersucht │ │ └── level2/ – Untersucht /home2/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ └── eicar.file – Untersucht

Bei einem aktualisierbaren Kernel-Modul können mithilfe von Masken festgelegte Ausnahmen anders funktionieren. Die folgende Tabelle zeigt nur die Unterschiede bei Ausnahmen durch Pfadmasken im Vergleich zur fanotify-Technologie.

Unterschiede bei mithilfe von Masken festgelegten Ausnahmen für ein aktualisierbares Kernel-Modul

Struktur	Ausnahme	Ergebnis
/home/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ ├── eicar.file │ │ └── level2/ /home2/ ├── eicar ├── eicar.txt ├── eicar.file └── test1/ │ ├── eicar │ ├── eicar.txt │ ├── eicar.file │ └── level1/ │ │ ├── eicar │ │ ├── eicar.txt │ │ └── eicar.file	/home/* Diese Pfadmaske schließt alle Objekte im Verzeichnis /home und in dessen Unterverzeichnissen aus.	/home/ ├── eicar – **Ausgeschlossen** ├── eicar.txt – **Ausgeschlossen** ├── eicar.file – **Ausgeschlossen** └── test1/ – Untersucht │ ├── eicar – **Ausgeschlossen** │ ├── eicar.txt – **Ausgeschlossen** │ ├── eicar.file – **Ausgeschlossen** │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ ├── eicar.file – Untersucht │ │ └── level2/ – Untersucht /home2/ ├── eicar – Untersucht ├── eicar.txt – Untersucht ├── eicar.file – Untersucht └── test1/ – Untersucht │ ├── eicar – Untersucht │ ├── eicar.txt – Untersucht │ ├── eicar.file – Untersucht │ └── level1/ – Untersucht │ │ ├── eicar – Untersucht │ │ ├── eicar.txt – Untersucht │ │ └── eicar.file – Untersucht

So fügen Sie Schutzausnahmen hinzu

So fügen Sie Schutzausnahmen in der Web Console hinzu

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Schutz vor bedrohlichen Dateien**.
5. Klicken Sie auf den Link **Untersuchungsausnahmen**.
6. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.

7. Aktivieren Sie die Kontrollkästchen für die Kriterien, die Sie für eine Schutzausnahme verwenden möchten:

   - **Datei- oder Ordnerpfad**. Geben Sie einen Datei- oder Verzeichnispfad oder eine Dateinamensmaske an. Um Pfade in Containern oder Images anzugeben, verwenden Sie Tags.

     Geben Sie für ein lokales Dateisystem einen Verzeichnispfad an (z. B. `/path/to/folder/`). Geben Sie für ein eingehängtes Dateisystem oder für alle remote eingehängten Dateisysteme eine Dateinamensmaske ein. Geben Sie für ein eingehängtes Dateisystem außerdem das Zugriffsprotokoll an (NFS, Samba oder benutzerdefiniert).

   - **Objekttyp**. Geben Sie den Namen der Bedrohung an.

   - **Objekt-Hash**. Geben Sie den SHA256-Hash des Objekts ein. Sie können auch eine Datei hinzufügen oder ein Ereignis angeben, aus dem der SHA256-Hash für die Ausnahme abgeleitet werden soll.

8. Wählen Sie die Schutzkomponenten aus, auf die Sie die Ausnahme anwenden möchten:

   - **Alle Schutzkomponenten**. Die Ausnahme wird auf alle Schutzkomponenten angewendet, die von **Ausnahmen für die Schadsoftware-Untersuchung** betroffen sind.

   - **Ausgewählte Schutzkomponenten**. Wählen Sie die Komponenten aus, auf die Sie die Ausnahme anwenden möchten: Schutz vor bedrohlichen Dateien, Schutz vor Verschlüsselung, Exploit-Prävention.

9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So fügen Sie Schutzausnahmen über die Befehlszeile hinzu

1. Führen Sie den folgenden Befehl aus, um eine Ausnahme nach Pfad hinzuzufügen:

   ```
   kesl-control --set-settings 1 --add-exclusion <path>
   ```

2. Um eine Ausnahme nach Maske hinzuzufügen, gehen Sie folgendermaßen vor:

   a. Aktivieren Sie Ausnahmen nach Dateimaske:

   ```
   kesl-control --set-settings 1 UseExcludeMasks=Yes
   ```

   b. Fügen Sie eine Dateimaske hinzu:

   ```
   kesl-control --set-settings 1 ExcludeMasks.item_#=<file mask>
   ```

3. Um eine Ausnahme nach dem Namen der Bedrohung hinzuzufügen, gehen Sie folgendermaßen vor:

   a. Aktivieren Sie Ausnahmen nach dem Namen der Bedrohung für Dateien:

   ```
   kesl-control --set-settings 1 UseExcludeThreats=Yes
   ```

   b. Fügen Sie einen Namen der Bedrohung hinzu:

   ```
   kesl-control --set-settings 1 ExcludeThreats.item_#=<threat name>
   ```

4. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 1
```

Symbole

Befehlsoptionen

Einstellung	Description
`--add-exclusion`	Verzeichnis von der Untersuchung ausschließen. Den Aufgabeneinstellungen wird ein neuer Abschnitt vom Typ `[ExcludedFromScanScope.item_#]` hinzugefügt. Die Anwendung schließt die Objekte im Verzeichnis, das im Parameter `path` angegeben ist, von der Untersuchung aus.
`ExcludeMasks.item_#`	Ausnahme von der Untersuchung von Objekten nach Name oder Maske. Verwenden Sie Masken im Shell-Format, um den Dateinamen einzugeben. Beispiel: `ExcludeMasks.item_0000=*_my_file_??.html`.
`ExcludeThreats.item_#`	Schließt Objekte nach dem Namen der in den Objekten gefundenen Bedrohungen von der Untersuchung aus. 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 verwenden, um Informationen über Ihr Netzwerk zu erhalten. 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. Beispiel: `ExcludeThreats.item_0000=EICAR-Test-*`.

So fügen Sie Schutzausnahmen in der Verwaltungskonsole hinzu

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.

   Das Fenster **Eigenschaften: <Policy name>** wird geöffnet.
3. Gehen Sie zu **Basisschutz** → **Ausnahmen für den Schutz vor bedrohlichen Dateien**.

So fügen Sie Ausnahmen nach Pfad hinzu:

1. Klicken Sie unter **Ausnahmen** auf **Konfigurieren**.

   Dadurch wird ein Fenster mit einer Tabelle der Ausnahmebereiche geöffnet.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Geben Sie den Namen des Ausnahmebereichs an, z. B. *Systemdateien*.
4. Geben Sie den Pfad zu einer einzelnen Datei oder einem Verzeichnis an (z. B. `/path/to/folder`). Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.
5. Geben Sie Masken für Objektnamen im Format der Befehlsshell an (z. B. `*.txt` oder `file?.*`). Fügen Sie Masken einzeln hinzu.
6. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie Ausnahmen nach Dateinamenmaske hinzu:

1. Klicken Sie unter **Ausnahmen nach Maske** auf die Schaltfläche **Konfigurieren**.

   Dadurch wird ein Fenster mit einer Tabelle der Ausnahmebereiche nach Maske geöffnet.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

3. Geben Sie die Dateinamenmaske im Format der Befehlsshell an (z. B. `*.txt` oder `file?.*`). Fügen Sie Masken einzeln hinzu.

4. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie Ausnahmen nach Bedrohungsname hinzu:

1. Klicken Sie im Block **Ausnahmen nach Bedrohungsname** auf **Konfigurieren**.

   Dadurch wird ein Fenster mit einer Tabelle der Ausnahmebereiche nach Bedrohungsname geöffnet.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

3. Geben Sie den Namen der Bedrohung an. Name des Objekttyps gemäß der Klassifikation der Kaspersky-Enzyklopädie (z. B. `Email-Worm`, `Rootkit` oder `RemoteAdmin`). Sie können den Namen einer Bedrohung mithilfe einer Maske angeben.

4. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie Ausnahmen nach Prozess hinzu:

1. Klicken Sie im Block **Ausnahmen nach Prozessen** auf **Konfigurieren**.

   Dadurch wird ein Fenster mit einer Tabelle der Ausnahmebereiche nach Prozess geöffnet.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Vertrauenswürdiger Prozess** wird geöffnet.

3. Geben Sie den Namen des Ausnahmebereichs an.

4. Geben Sie den vollständigen Pfad zum ausgeschlossenen Prozess an.

5. Aktivieren Sie bei Bedarf das Kontrollkästchen **Auf untergeordnete Prozesse anwenden**. Das Programm schließt untergeordnete Prozesse des ausgeschlossenen Prozesses von der Untersuchung aus.

6. Aktivieren Sie das Kontrollkästchen **Diesen Bereich verwenden**. Das Programm schließt diesen Bereich von Untersuchungen aus. Dieses Kontrollkästchen ist standardmäßig aktiviert.

7. Wählen Sie unter **Pfad zu den geänderten Dateien** den Typ des Dateisystems aus, in dem sich die von Untersuchungen auszuschließenden Verzeichnisse befinden:

   - **Lokal** für lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie den Pfad zu einem lokalen Verzeichnis angeben.
   - **Mounted** für eingebundene Remote- oder lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie das Protokoll oder den Namen des Dateisystems angeben.
   - **Freigegeben** für Dateisystemressourcen des geschützten Servers, die über das Samba- oder NFS-Protokoll zugänglich sind.
   - **Alle remote-mounted** für alle Remote-Verzeichnisse, die auf dem Gerät über das Samba- und das NFS-Protokoll eingebunden sind.
   - **Alle freigegebenen** für alle Dateisystemressourcen des geschützten Servers, die über das Samba- und das NFS-Protokoll zugänglich sind.

8. Geben Sie Masken für Objektnamen im Format der Befehlsshell an (z. B. `*.txt` oder `file?.*`). Fügen Sie Masken einzeln hinzu.

9. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie vertrauenswürdige Webadressen hinzu

Der „Schutz vor Web-Bedrohungen“ kann nicht nur bösartige Websites und Phishing-Websites blockieren. Beispielsweise blockiert der „Schutz vor Web-Bedrohungen“ auch HTTP-Datenverkehr, der nicht den RFC-Standards entspricht. Sie können eine Liste der Webadressen anlegen, deren Inhalt Sie vertrauen. Informationen, die von vertrauenswürdigen Webadressen stammen, werden von der Komponente „Schutz vor Web-Bedrohungen“ nicht auf Viren und andere gefährliche Programme analysiert. Diese Option kann beispielsweise nützlich sein, wenn die Komponente „Schutz vor Web-Bedrohungen“ den Download einer Datei von einer Ihnen bekannten Website verhindert.

So fügen Sie in der Web Console eine vertrauenswürdige Webadresse hinzu

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wechseln Sie zum Abschnitt **Vertrauenswürdige Zone**.

5. Klicken Sie im folgenden Fenster auf den Link **Webadressen**.

   Daraufhin wird ein Fenster mit einer Liste vertrauenswürdiger Webadressen geöffnet.

6. Erstellen Sie eine Liste mit Adressen der Websites / Webseiten, deren Inhalt Sie vertrauen.

   Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

   Außerdem können Sie eine Liste mit vertrauenswürdigen Webadressen aus einer JSON-Datei importieren.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So fügen Sie eine vertrauenswürdige Webadresse über die Befehlszeile hinzu

1. Führen Sie den folgenden Befehl aus, um die Liste der vertrauenswürdigen Webadressen zu aktivieren:

```
kesl-control --set-settings 14 UseTrustedAddresses=Yes
```

2. Führen Sie den folgenden Befehl aus, um eine vertrauenswürdige Webadresse hinzuzufügen:

```
kesl-control --set-settings 14 TrustedAddresses.item_#=<trusted web address>
```

3. Um die aktuellen Werte der Komponenteneinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 14
```

Beispiel

```
kesl-control --set-settings 14 TrustedAddresses.item_001=https://example.com/
```

So fügen Sie eine vertrauenswürdige IP-Adresse eines Computers hinzu

Kaspersky Endpoint Security kann einen Netzwerkangriff erkennen und eine ungesicherte Netzwerkverbindung blockieren, die eine große Anzahl von Paketen (z. B. von Überwachungskameras) überträgt. Um mit vertrauenswürdigen Geräten zu arbeiten, können Sie die IP-Adressen dieser Geräte zu der Liste der Ausnahmen hinzufügen. Vertrauenswürdige Webadressen wirken sich auf die Komponente Schutz vor Netzwerkbedrohungen aus.

So konfigurieren Sie in der Web Console Adressen, die von der Blockierung ausgeschlossen sind

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Vertrauenswürdige Zone**.
5. Klicken Sie im folgenden Fenster auf den Link **IP-Adressen**.

   Daraufhin wird ein Fenster mit einer Liste vertrauenswürdiger IP-Adressen geöffnet.
6. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.
7. Geben Sie die IP-Adresse des Computers ein, der blockiert werden soll, wenn Netzwerkangriffe von ihm ausgehen.

   Geben Sie bei Bedarf das Subnetz an.
8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie über die Befehlszeile Adressen, die von der Blockierung ausgeschlossen sind

1. Führen Sie den folgenden Befehl aus, um vertrauenswürdige IP-Adressen zu übernehmen:

   ```
   kesl-control --set-settings 17 UseExcludeIPs=Yes
   ```
2. Führen Sie den folgenden Befehl aus, um eine vertrauenswürdige IP-Adresse hinzuzufügen:

   ```
   kesl-control --set-settings 17 ExcludeIPs.item_#=<IP address>
   ```

3. Führen Sie den folgenden Befehl aus, um die Liste der vertrauenswürdigen IP-Adressen zu überprüfen:

```
kesl-control --get-settings 17 TrustedIPAddresses
```

Beispiel

```
kesl-control --set-settings 17 ExcludeIPs.item_0000="192.168.2.0/24"
```

So wählen Sie überwachte Netzwerkports aus

Kaspersky Endpoint Security überwacht Datenströme, die über bestimmte Protokolle übertragen werden und bestimmte offene TCP-Ports auf dem Computer des Benutzers passieren. Standardmäßig überwacht die Anwendung bekannte und registrierte Ports, beispielsweise Port 443 für HTTPS-Verbindungen und Port 143 für das E-Mail-Protokoll IMAP.

Vertrauenswürdige Netzwerkports sind Netzwerkports, die von der Komponente Schutz vor Netzwerkbedrohungen von der Untersuchung ausgeschlossen werden. Dies ist erforderlich, um Kaspersky Endpoint Security für die Kompatibilität mit vertrauenswürdigen Diensten und Anwendungen von Drittanbietern zu konfigurieren und die Leistung zu optimieren. Sie können beispielsweise Netzwerkports für interne Backup-Dienste angeben, damit die Anwendung das Herunterladen oder Hochladen von Backup-Kopien nicht beeinträchtigt.

Beachten Sie, dass ein Gerät weniger geschützt ist, wenn Netzwerkports von der Untersuchung ausgeschlossen werden. Versuchen Sie, die Ausnahmen auf ein Minimum zu beschränken.

Netzwerkports in der Web Console von der Untersuchung ausschließen

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Vertrauenswürdige Zone** → **Netzwerkports**.

   Dadurch wird ein Fenster mit einer Liste der überwachten Netzwerkports geöffnet.
5. Deaktivieren Sie den Umschalter für die Ports, die Sie von der Untersuchung ausschließen möchten.

   Wenn der benötigte Port nicht aufgeführt ist, bedeutet dies, dass die Anwendung diesen Port nicht untersucht.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Netzwerkports über die Befehlszeile von der Untersuchung ausschließen

1. Rufen Sie eine Liste der überwachten Ports ab, indem Sie den folgenden Befehl ausführen:

```
kesl-control --get-net-setting
```

2. Wenn die Überwachung aller Ports aktiviert ist (`MonitorNetworkPorts=All`), führen Sie den folgenden Befehl aus:

   ```
   kesl-control --set-net-settings MonitorNetworkPorts=Selected
   ```

   Dadurch wird ein `[NetworkPorts.item_#]`-Abschnitt hinzugefügt, der überwachte Netzwerkports enthält.

3. Wenn der Abschnitt einen Port enthält, den Sie von der Untersuchung ausschließen möchten, gehen Sie folgendermaßen vor:

   a. Um die Einstellungen für die Untersuchung des Netzwerkverkehrs in eine Datei auszugeben, führen Sie den folgenden Befehl aus:

      ```
      kesl-control --get-net-setting --file <path to file>
      ```

   b. Löschen Sie in dieser Datei die `[NetworkPorts.item_#]`-Abschnitte, die Netzwerkports enthalten, die nicht überwacht werden sollen.

   c. Um Ihre Einstellungen zu übernehmen, führen Sie den folgenden Befehl aus:

      ```
      kesl-control --set-net-settings --file <path to file>
      ```

      Die geänderten Einstellungen werden in die Anwendung importiert.

So fügen Sie ein Zertifikat zur Liste der vertrauenswürdigen Stammzertifikate hinzu

Mit Kaspersky Endpoint Security können Sie vertrauenswürdige Stammzertifikate auf Benutzercomputern installieren, beispielsweise um eine neue Zertifizierungsstelle bereitzustellen. Sie können ein Zertifikat zu einem speziellen Zertifikatspeicher von Kaspersky Endpoint Security hinzufügen. In diesem Fall wird das Zertifikat nur für das Programm Kaspersky Endpoint Security als vertrauenswürdig betrachtet. Anders gesagt: Der Benutzer kann über das neue Zertifikat im Browser auf eine Website zugreifen. Wenn ein anderes Programm versucht, auf die Website zuzugreifen, erhalten Sie möglicherweise einen Verbindungsfehler aufgrund eines Zertifikatfehlers.

Vertrauenswürdige Stammzertifikate werden von den folgenden Komponenten verwendet:

- Schutz vor Web-Bedrohungen
- Schutz vor E-Mail-Bedrohungen
- Web-Kontrolle

Vertrauenswürdige Zertifikate in den Formaten CER, CRT, PEM und DER werden unterstützt. Die maximale Dateigröße für ein vertrauenswürdiges Zertifikat beträgt 2 MB.

So installieren Sie ein vertrauenswürdiges Stammzertifikat in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Vertrauenswürdige Zone** → **Stammzertifikate**.
   Dies öffnet ein Fenster mit einer Liste der vertrauenswürdigen Stammzertifikate.
5. Klicken Sie auf die Schaltfläche **Hinzufügen**.
   Das Formular zum Hinzufügen eines Zertifikats wird geöffnet.
6. Laden Sie das Zertifikat hoch.
7. Geben Sie bei Bedarf im Feld **Kommentar** eine Beschreibung des Zertifikats ein.
8. Speichern Sie die vorgenommenen Änderungen.

In der Liste der vertrauenswürdigen Zertifikate wird die Seriennummer als Zertifikatsname verwendet.

So installieren Sie ein vertrauenswürdiges Stammzertifikat über die Befehlszeile

1. Um ein Zertifikat hinzuzufügen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --add-certificate <path to certificate>
   ```

2. Um die Liste der vertrauenswürdigen Stammzertifikate anzuzeigen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --list-certificates
   ```

   Für jedes Zertifikat werden folgende Daten angezeigt:

   - Zertifikatinhaber
   - Seriennummer
   - Zertifikataussteller
   - Beginn der Gültigkeitsdauer des Zertifikats
   - Ende der Gültigkeitsdauer des Zertifikats
   - SHA256-Fingerabdruck des Zertifikats

3. Um ein Zertifikat aus der Liste zu entfernen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --remove-certificate <certificate subject>
   ```

So fügen Sie eine vertrauenswürdige Domäne hinzu

Kaspersky Endpoint Security verfügt über eine Liste vertrauenswürdiger Domänen, für die verschlüsselte Verbindungen nicht untersucht werden. Vertrauenswürdige Domänen wirken sich auf Schutz vor Web-Bedrohungen und Web-Kontrolle aus. Durch das Ausschließen von Domänen von der Untersuchung können Sie verhindern, dass Datenverkehr aus Ihnen bekannten Quellen blockiert wird.

Geben Sie den Domain-Namen an. Webadressen wie `example.com/*` oder `https://example.com` werden ignoriert.

So geben Sie vertrauenswürdige Domänen in der Web Console an

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Vertrauenswürdige Zone** → **Vertrauenswürdige Domänen**.
   Dies öffnet ein Fenster mit einer Liste vertrauenswürdiger Domänen.
5. Klicken Sie auf die Schaltfläche **Hinzufügen**.
   Das Formular zum Hinzufügen einer Domäne wird geöffnet.
6. Geben Sie einen Domänennamen oder eine Domänenmaske an. Beispiel: `*example.com`.
7. Speichern Sie die vorgenommenen Änderungen.

So geben Sie vertrauenswürdige Domänen in der Befehlszeile an

1. Um eine Domäne hinzuzufügen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --set-net-settings ManageExclusions=Yes Exclusions.item_#.DomainName=<domain name>
   ```

2. Um Ihre Einstellungen zu testen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --get-net-settings
   ```

   Vertrauenswürdige Domänen sollten im Abschnitt `[Exclusions.item_#]` aufgeführt sein.

Beispiel

```
kesl-control --set-net-settings Exclusions.item_0000.DomainName=example.com
```

So schließen Sie Mount-Punkte aus

Um die Dateien eines bestimmten Verzeichnisses nicht nur von der Untersuchung, sondern auch vom Abfangen auszuschließen, müssen Sie den gesamten Mountpunkt ausschließen. Solche Ausnahmen werden als *globale Ausnahmen* bezeichnet. Das Programm schließt vertrauenswürdige lokale oder Remote-Verzeichnisse, die auf dem Gerät eingehängt sind, von der Untersuchung und dem Abfangen von Dateivorgängen aus. Sie können beispielsweise Mountpunkte ausschließen, die temporäre Dateien enthalten, um die Systemlast zu verringern und Untersuchungen schneller abzuschließen.

Ausnahmen für Mountpunkte wirken sich auf die folgenden Komponenten aus:

- Schutz vor bedrohlichen Dateien
- Schutz vor Verschlüsselung
- Container untersuchen

Vertrauenswürdige Mountpunkte werden außerdem von der Untersuchung durch die folgenden Aufgaben ausgeschlossen:

- Schadsoftware-Untersuchung.
- Untersuchung wichtiger Bereiche.
- Container untersuchen
- Untersuchung von Wechseldatenträgern

Die Mountpunkte müssen genau so angegeben werden, wie sie in der Ausgabe des Befehls `mount` angezeigt werden.

So geben Sie vertrauenswürdige Mountpunkte in der Web Console an

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Vertrauenswürdige Zone** → **Mount-Points**.

   Daraufhin wird ein Fenster mit einer Liste der vertrauenswürdigen Mountpunkte geöffnet.
5. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Daraufhin wird das Formular zum Hinzufügen eines Mountpunkts geöffnet.
6. Wählen Sie in der Dropdown-Liste der Dateisysteme den Typ des Dateisystems aus, auf dem sich die auszuschließenden Verzeichnisse befinden: **Lokal**, **Eingehängt**, **Alle remote eingehängten**.

   Kaspersky Endpoint Security unterstützt die Protokolle Samba und NFS für Remote-Verzeichnisse.

Die Mountpunkte müssen genau so angegeben werden, wie sie in der Ausgabe des Befehls `mount` angezeigt werden.

7. Geben Sie den Namen des Dateisystems ein, das die auszuschließenden Verzeichnisse enthält.
8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So geben Sie vertrauenswürdige Mountpunkte über die Befehlszeile an

1. Wenn das Verzeichnis kein Mountpunkt ist, erstellen Sie daraus einen Mountpunkt, indem Sie folgenden Befehl ausführen:

```
mount --bind <path to dir> <path to dir>
```

2. Tragen Sie in die Datei `/etc/fstab` die folgende Zeile ein, damit der Mountpunkt nach dem Neustart des Servers erhalten bleibt:

```
<path to dir> <path to dir> none defaults,bind 0 0
```

3. Starten Sie Kaspersky Endpoint Security neu:

```
systemctl restart kesl
```

4. Führen Sie den folgenden Befehl aus, um einen vertrauenswürdigen Mountpunkt hinzuzufügen:

```
kesl-control --set-app-settings ExcludedMountPoint.item_#=<path to mount point>
```

5. Starten Sie die Anwendung neu, um die globalen Ausnahmen anzuwenden:

```
systemctl restart kesl
```

Beispiel

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/tmp"
```

So fügen Sie vertrauenswürdige Programme hinzu

Die *Liste der vertrauenswürdigen Programme* ist eine Liste mit Programmen, für die Kaspersky Endpoint Security weder die Datei- und Prozessaktivität (einschließlich schädlicher Aktivität) noch den Prozessspeicher überwacht. Kaspersky Endpoint Security überwacht standardmäßig alle Objekte, die von einem beliebigen Programmprozess geöffnet, gestartet oder gespeichert werden, und kontrolliert die Aktivität aller Programme.

Vertrauenswürdige Programme wirken sich auf die folgenden Komponenten aus:

- Schutz vor bedrohlichen Dateien
- Verhaltensanalyse

Sowie Ausnahmen von der Untersuchung des Prozessspeichers.

So geben Sie vertrauenswürdige Programme in der Web Console an

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Vertrauenswürdige Zone** → **Vertrauenswürdige Programme**.

   Dies öffnet ein Fenster mit einer Liste von vertrauenswürdigen Programmen.
5. Aktivieren Sie das Kontrollkästchen **Bei Vererbung Werte zusammenführen**, wenn Sie eine konsolidierte Liste der vertrauenswürdigen Programme für alle Computer des Unternehmens erstellen möchten. Die Listen mit vertrauenswürdigen Programmen der übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Programme aus der übergeordneten Richtlinie werden in untergeordneten Richtlinien nur zur Ansicht angezeigt. Sie können nicht geändert oder gelöscht werden.

   > Um Listen zusammenzuführen, muss die Vererbung der übergeordneten Richtlinieneinstellungen aktiviert sein.
6. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Formular zum Hinzufügen eines Programms wird geöffnet.
7. Geben Sie den Pfad zum Programm oder eine Pfadmaske an.
8. Konfigurieren Sie die Einstellungen für vertrauenswürdige Programme:

   - **Dateien, die dieses Programm öffnet, nicht untersuchen**. Alle Dateien, die vom Programm geöffnet werden, sind von der Überprüfung durch Kaspersky Endpoint Security ausgeschlossen.
   - **Programmaktivität nicht überwachen**. Kaspersky Endpoint Security überwacht die Datei- und Netzwerkaktivität eines vertrauenswürdigen Programms im Betriebssystem nicht.

     Sie können die Überwachung der Programmaktivität auch separat für die Komponenten MDR und EDR (KATA) konfigurieren, indem Sie das Kontrollkästchen **Nicht überwachen für Managed Detection and Response und Endpoint Detection and Response** aktivieren.
   - **Aktivität von Unterprogrammen nicht überwachen**. Kaspersky Endpoint Security überwacht die Datei- und Netzwerkaktivität von Programmen nicht, die von einem vertrauenswürdigen Programm gestartet werden.
   - **Speicher des angegebenen Programms nicht untersuchen**. Kaspersky Endpoint Security untersucht den Speicher von Prozessen nicht, die von einem vertrauenswürdigen Programm erzeugt wurden.

In der Web Console ist die Einstellung **Kommentar** für Kaspersky Endpoint Security für Linux nicht verfügbar.

9. Speichern Sie die vorgenommenen Änderungen.

So geben Sie vertrauenswürdige Programme in der Befehlszeile an

1. Um die Dateiaktivität eines vertrauenswürdigen Programms von der Untersuchung auszuschließen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 1 ExcludedForProgram.item_#.UseExcludedForProgram=Yes
ExcludedForProgram.item_#.ProgramPath=<path to app> ExcludedForProgram.item_#.AreaDesc=<trusted app name>
[ExcludedForProgram.item_#.ApplyToDescendants=Yes]
```

2. Um die Prozessaktivität eines vertrauenswürdigen Programms von der Untersuchung auszuschließen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-set 20 UseTrustedPrograms=Yes TrustedPrograms.item_#.UseTrustedProgram=Yes
TrustedPrograms.item_#.ProgramPath=<path to app> TrustedPrograms.item_#.ProgramDesc=<trusted app name>
[TrustedPrograms.item_#.UseTrustedProgramForMDRAndEDR=Yes] [TrustedPrograms.item_#.ApplyToDescendants=Yes]
```

3. Um den Speicher der Prozesse eines vertrauenswürdigen Programms von der Untersuchung auszuschließen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings MemScanExcludedProgramPath.item_#=<path to app>
```

Symbole

Befehlsoptionen

Parameter	Description
`ExcludedForProgram.item_#.UseExcludedForProgram=Yes`	Schließt die Dateiaktivität eines vertrauenswürdigen Programms von der Untersuchung durch die Komponente „Schutz vor bedrohlichen Dateien“ aus.
`ExcludedForProgram.item_#.ProgramPath`	Pfad zum vertrauenswürdigen Programm mit ID `#`. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht die Prozesse des angegebenen Programms nicht. Wenn für das Abfangen von Systemereignissen das aktualisierbare Kernel-Modul verwendet wird, wird der angegebene Prozess in allen Namensräumen vom Abfangen ausgeschlossen.
`ExcludedForProgram.item_#.AreaDesc`	Name des vertrauenswürdigen Programms mit ID `#`.
`ExcludedForProgram.item_#.ApplyToDescendants=Yes`	Schließt untergeordnete Prozesse eines vertrauenswürdigen Programms von der Untersuchung durch die Komponente „Schutz vor bedrohlichen Dateien“ aus.
`UseTrustedPrograms=Yes`	Schließt die Aktivität von Prozessen vertrauenswürdiger Programme von der Untersuchung durch die Komponente „Verhaltensanalyse“ aus.
`TrustedPrograms.item_#.UseTrustedProgram=Yes`	Schließt die Aktivität eines vertrauenswürdigen Programms mit ID `#` von der Untersuchung aus.

Parameter	Description
`TrustedPrograms.item_#.ProgramPath`	Pfad zum vertrauenswürdigen Programm mit ID `#`. Die Komponente „Verhaltensanalyse“ untersucht die Prozesse des angegebenen Programms nicht. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.
`TrustedPrograms.item_#.ProgramDesc`	Name des vertrauenswürdigen Programms mit ID `#`.
`TrustedPrograms.item_#.UseTrustedProgramForMDRAndEDR=Yes`	Schließt die Aktivität eines vertrauenswürdigen Programms von der Erfassung von Telemetriedaten durch die Komponenten „Managed Detection and Response“ und „Endpoint Detection and Response Expert (on-premise)“ aus.
`TrustedPrograms.item_#.ApplyToDescendants=Yes`	Schließt untergeordnete Prozesse eines vertrauenswürdigen Programms von der Untersuchung durch die Komponente „Verhaltensanalyse“ aus.
`MemScanExcludedProgramPath.item_#`	Pfad zum vertrauenswürdigen Programm mit ID `#`. Das Programm überprüft den Speicher der Prozesse des vertrauenswürdigen Programms nicht.

So fügen Sie vertrauenswürdige Geräte hinzu

Vertrauenswürdige Geräte sind Geräte, auf die jene Benutzer, die in den Einstellungen eines vertrauenswürdigen Gerätes angegeben sind, jederzeit vollständigen Zugriff besitzen.

Sie können entweder einem einzelnen Benutzer, einer Benutzergruppe oder allen Benutzern des Unternehmens den Zugriff auf vertrauenswürdige Geräte gewähren. Wenn in Ihrem Unternehmen beispielsweise die Verwendung von Wechseldatenträgern verboten ist, aber die Administratoren für ihre Arbeit Wechseldatenträger verwenden, können Sie die Verwendung von Wechseldatenträgern nur für die Gruppe der Administratoren erlauben. Dazu müssen Wechseldatenträger zur Liste der vertrauenswürdigen Geräte hinzugefügt werden und die Zugriffsrechte für Benutzer angepasst werden.

Sie können vertrauenswürdige Geräte mithilfe der folgenden Daten hinzufügen:

- **ID**. Jedes Gerät besitzt eine eindeutige Kennung (Hardware ID oder HWID). Die ID finden Sie mithilfe von Betriebssystem-Tools in den Eigenschaften des Gerätes. Beispiel für eine Geräte-ID: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Es bietet sich an, Geräte mithilfe von IDs hinzuzufügen, wenn Sie mehrere bestimmte Geräte hinzufügen möchten.

- **Nach ID-Maske**. Wenn Sie mehrere Geräte mit ähnlichen IDs verwenden, können Sie Masken verwenden, um die Geräte zur Liste der vertrauenswürdigen Geräte hinzuzufügen. Das Zeichen `*` steht als Platzhalter für eine beliebige Zeichenkombination. Das Zeichen `?` steht als Platzhalter für ein beliebiges Einzelzeichen. Beispiel: `WDC_C*`.

So fügen Sie vertrauenswürdige Geräte in der Kaspersky Security Center Web Console hinzu

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Gerätekontrolle** → **Vertrauenswürdige Geräte**.

   Dadurch wird ein Fenster mit einer Liste der vertrauenswürdigen Geräte geöffnet.

5. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Daraufhin wird das Formular zum Hinzufügen eines Geräts geöffnet.

6. Geben Sie unter **Benutzer oder Gruppe** einen Benutzer oder eine Benutzergruppe an, für den bzw. die das Gerät als vertrauenswürdig gelten soll.

   Sie können Benutzer in der Liste der Benutzerkonten in Kaspersky Security Center auswählen oder einen lokalen Benutzernamen manuell eingeben. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

   Für die Gruppe „Jeder“ ist der Zugriff auf vertrauenswürdige Geräte standardmäßig erlaubt.

7. Wählen Sie unter **Gerätetyp** in der Dropdown-Liste einen Gerätetyp aus (z. B. **Wechseldatenträger**).

8. Wenn Sie ein Gerät anhand einer ID-Maske hinzufügen möchten, aktivieren Sie das Kontrollkästchen **Maske verwenden**.

9. Geben Sie im Feld **Suche nach vertrauenswürdigen Geräten** eine Geräte-ID oder ID-Maske ein.

   In der Tabelle wird eine Liste der Geräte angezeigt, die den angegebenen Kriterien entsprechen.

10. Aktivieren Sie die Kontrollkästchen für jene Geräte, die zur Liste der vertrauenswürdigen Geräte hinzugefügt werden sollen.

11. Beschreiben Sie bei Bedarf auf der Registerkarte **Kommentar** den Grund, warum die Geräte zur Liste der vertrauenswürdigen Geräte hinzugefügt wurden.

12. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So fügen Sie vertrauenswürdige Geräte über die Befehlszeile hinzu

1. Führen Sie den folgenden Befehl aus, um vertrauenswürdige Geräte hinzuzufügen:

   ```
   kesl-control --trusted-devices --add <device ID>
   ```

2. Führen Sie den folgenden Befehl aus, um die Liste der vertrauenswürdigen Geräte der Komponente zu durchsuchen:

   ```
   kesl-control --trusted-devices --list
   ```

Beispiel

```
kesl-control --trusted-devices --add WDC_C*
```

Allgemeine Einstellungen

Konfiguration der Erkennung

Erkennen sonstiger Objekttypen

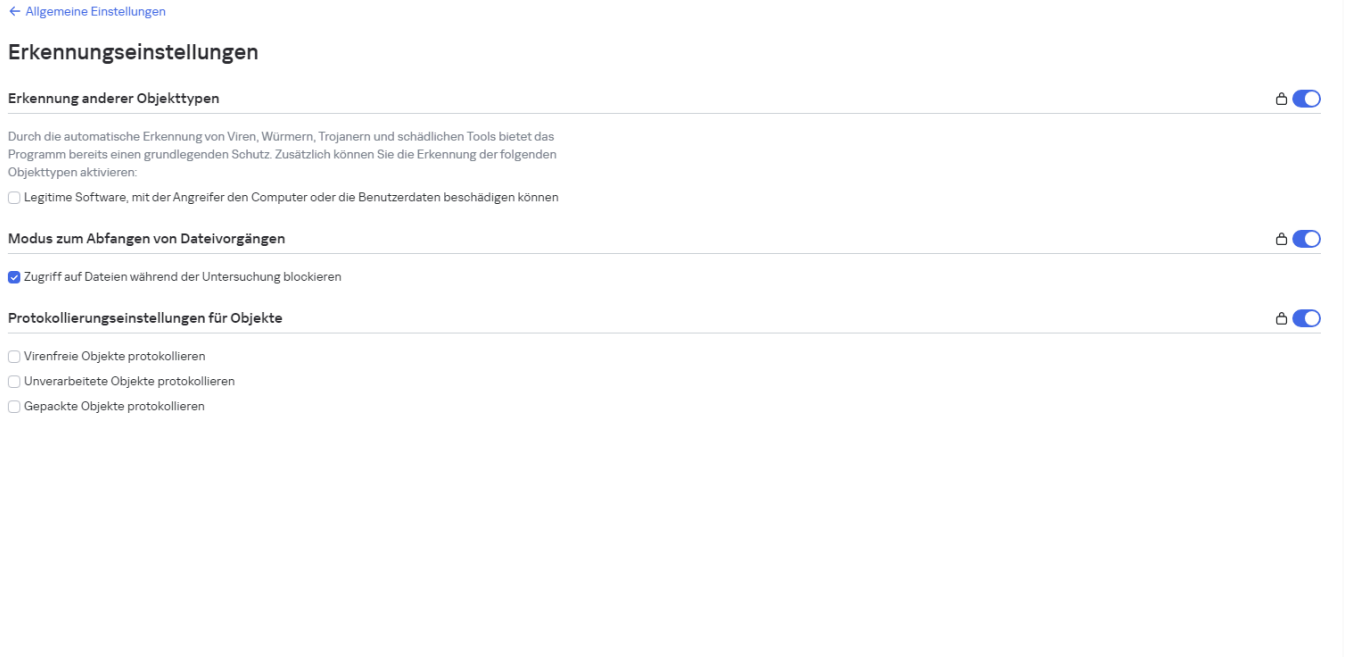
Kaspersky Endpoint Security sucht unabhängig von den aktuellen Einstellungen stets nach Viren, Würmern und Trojanern und blockiert diese. Diese Programme können dem Computer erheblichen Schaden zufügen.

Zusätzlich können Sie die Erkennung von legitimen Anwendungen aktivieren, die von Angreifern für Kompromittierungen von Computern oder Benutzerdaten ausgenutzt werden können. Diese Anwendungen selbst verfolgen nicht unbedingt einen schädlichen Zweck, können aber von Angreifern ausgenutzt werden. Ausführliche Informationen zu legitimen Anwendungen, die von Angreifern für Kompromittierungen des Computers oder der Benutzerdaten ausgenutzt werden können, finden Sie auf der Website von Kaspersky Encyclopedia.

So konfigurieren Sie die Erkennung von Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können, in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Erkennungseinstellungen**.
5. Aktivieren Sie im Block **Erkennung anderer Objekttypen** das Kontrollkästchen **Legitime Software, mit der Angreifer den Computer oder die Benutzerdaten beschädigen können**.
6. Speichern Sie die vorgenommenen Änderungen.



So konfigurieren Sie die Erkennung von Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können, über die Befehlszeile

1. Um die Erkennung von Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können, zu konfigurieren, führen Sie den folgenden Befehl für die Schutzkomponenten des Programms aus:

   ```
   kesl-control --set-app-settings DetectOtherObjects=<Yes|No>
   ```

2. Um Links mit der Datenbank für Webadressen abzugleichen, die legitime Anwendungen enthalten, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können, führen Sie in der Komponente Schutz vor Web-Bedrohungen den folgenden Befehl aus:

   ```
   kesl-control --set-settings 14 CheckOther=<Yes|No>
   ```

3. Um die aktuellen Anwendungseinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --get-app-settings
   ```

4. Um die aktuellen Einstellungen für Schutz vor Web-Bedrohungen zu überprüfen, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --get-settings 14
   ```

Einstellungen für die Ereignisprotokollierung

Standardmäßig protokolliert Kaspersky Endpoint Security weder Ereignisse zur Verarbeitung gepackter und nicht infizierter Objekte noch Ereignisse zu Objekten, die von der Komponente Schutz vor bedrohlichen Dateien nicht verarbeitet wurden.

Sie können die Protokollierung solcher Ereignisse aktivieren, damit das Programm die Ereignisse *Gepacktes Objekt erkannt*, *Objekt nicht verarbeitet* und *Objekt wird verarbeitet* generiert. Solche Ereignisse können bei der Konfiguration der Komponente sowie beim Debugging oder bei der Fehlerbehebung des Programms nützlich sein. So können Sie sicherstellen, dass solche Objekte vom Programm untersucht und nicht aufgrund von Fehlern übersprungen wurden.

So aktivieren Sie die Protokollierung von Ereignissen über die Objektverarbeitung in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Erkennungseinstellungen**.

5. Unter **Protokollierungseinstellungen für Objekte** aktivieren Sie die Kontrollkästchen neben den relevanten Ereignistypen.
   - **Virenfreie Objekte protokollieren**
   - **Unverarbeitete Objekte protokollieren**
   - **Gepackte Objekte protokollieren**
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie mithilfe der Befehlszeile die Protokollierung von Ereignissen über die Verarbeitung von Objekten

1. Um Ereignisse über nicht infizierte Objekte zu protokollieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 1 ReportCleanObjects=Yes
```

2. Um Ereignisse über nicht verarbeitete Objekte zu protokollieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 1 ReportUnprocessedObjects=Yes
```

3. Um Ereignisse über gepackte Objekte zu protokollieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 1 ReportPackedObjects=Yes
```

4. Um die aktuellen Werte der Einstellungen für Schutz vor bedrohlichen Dateien zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 1
```

Kaspersky Security Network

Um Benutzercomputer effektiver zu schützen, verwendet Kaspersky Endpoint Security die von Benutzern aus aller Welt empfangenen Daten. Für den Empfang dieser Daten ist Kaspersky Security Network vorgesehen.

Die Funktionen für KSN sind in dieser Anwendung in den USA möglicherweise nicht verfügbar.

Kaspersky Security Network (KSN) ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf die Kaspersky-Online-Wissensdatenbank bietet, die Informationen über die Reputation von Dateien, Webressourcen und Software enthält. Durch die Verwendung der Daten aus dem Kaspersky Security Network wird die Reaktion von Kaspersky Endpoint Security auf unbekannte Bedrohungen beschleunigt, die Leistungsfähigkeit einiger Komponenten erhöht und das Risiko von Fehlalarmen reduziert. Wenn Sie an Kaspersky Security Network teilnehmen, erhält Kaspersky Endpoint Security von den KSN-Diensten Informationen über die Reputation untersuchter Webadressen sowie Informationen über die Kategorie und Reputation untersuchter Dateien. Weitere Informationen über die KSN-Konfiguration finden Sie in der Hilfe zu Kaspersky Security Center.

Die Verwendung von Kaspersky Security Network ist freiwillig. Das Programm schlägt während der Erstkonfiguration des Programms vor, KSN zu verwenden. Die KSN-Nutzung kann jederzeit begonnen oder beendet werden.

Detaillierte Informationen über den Versand an Kaspersky, 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 Seite von Kaspersky. Die Datei ksn_license.<language ID> mit dem Text der Erklärung zu Kaspersky Security Network ist im Distributionspaket des Programms enthalten und im Verzeichnis /opt/kaspersky/kesl/doc verfügbar.

Die Infrastruktur der Kaspersky-Reputationsdatenbanken

Kaspersky Endpoint Security unterstützt die folgenden Infrastrukturlösungen für die Verwendung der Reputationsdatenbanken von Kaspersky:

- Die Lösung *Kaspersky Security Network (KSN)* wird von den meisten Kaspersky-Programmen verwendet. Die KSN-Teilnehmer erhalten Informationen von Kaspersky und senden an Kaspersky bestimmte Informationen über Objekte, die auf dem Benutzercomputer gefunden wurden. Auf diese Weise können die Daten zusätzlich durch die Kaspersky-Analysten untersucht werden, um die Reputations- und Statistik-Datenbanken zu ergänzen.

- Die Lösung *Kaspersky Private Security Network (KPSN)* ermöglicht Benutzern den Zugriff auf die Kaspersky-Reputationsdatenbanken und auf andere statistische Daten, ohne dabei Daten von den Benutzercomputern an Kaspersky zu senden. Auf diesen Computern müssen Kaspersky Endpoint Security oder andere Kaspersky-Programme installiert sein. KPSN wurde für Unternehmenskunden entwickelt, die z. B. aus folgenden Gründen keine Möglichkeit zur Teilnahme an Kaspersky Security Network haben:

  - Lokale Arbeitsplätze haben keinen Internetzugriff.

  - 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 Anwendung 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 nicht möglich.

Einschränkungen von Kaspersky Private Security Network

Mit Kaspersky Private Security Network können Sie Ihre eigene lokale Reputationsdatenbank verwenden, um die Reputation von Objekten (Dateien oder Webadressen) zu überprüfen. Die Reputation eines Objekts, das der lokalen Reputationsdatenbank hinzugefügt wird, hat eine höhere Priorität als ein Objekt, das dem KSN/KPSN hinzugefügt wird. Stellen Sie sich zum Beispiel vor, Kaspersky Endpoint Security untersucht einen Computer und fordert die Reputation einer Datei im KSN/KPSN an. Wenn die Datei in der lokalen Reputationsdatenbank als *Nicht vertrauenswürdig* verzeichnet ist, in KSN/KPSN aber als *Vertrauenswürdig*, betrachtet Kaspersky Endpoint Security die Datei als *Nicht vertrauenswürdig* und führt die für erkannte Bedrohungen vorgesehene Aktion aus.

In einigen Fällen fordert Kaspersky Endpoint Security jedoch möglicherweise nicht die Reputation eines Objekts im KSN/KPSN an. Wenn dies der Fall ist, empfängt Kaspersky Endpoint Security keine Daten aus der lokalen Reputationsdatenbank von KPSN. Kaspersky Endpoint Security fragt aus folgenden Gründen möglicherweise nicht nach der Reputation eines Objekts im KSN/KPSN:

- Kaspersky-Programme verwenden Offline-Reputationsdatenbanken. Offline-Reputationsdatenbanken wurden entwickelt, um die Ressourcen während des Betriebs von Kaspersky-Programmen zu optimieren und kritisch wichtige Objekte auf dem Computer zu schützen. Offline-Reputationsdatenbanken werden von Kaspersky-Experten auf der Grundlage von Daten aus dem Kaspersky Security Network erstellt. Kaspersky-Programme aktualisieren Offline-Reputationsdatenbanken mit Antiviren-Datenbanken des jeweiligen Programms. Wenn Offline-Reputationsdatenbanken Informationen über ein untersuchtes Objekt enthalten, fordert das Programm die Reputation dieses Objekts nicht vom KSN/KPSN an.

- Untersuchungsausnahmen (vertrauenswürdige Zone) werden in den Programmeinstellungen konfiguriert. Wenn dies der Fall ist, berücksichtigt der Antrag die Reputation des Objekts in der lokalen Reputationsdatenbank nicht.

- Das Programm verwendet Technologien zur Untersuchungsoptimierung, wie iChecker oder das Zwischenspeichern von Reputationsanfragen an KSN / KPSN. Wenn dies der Fall ist, fordert das Programm möglicherweise nicht die Reputation von zuvor untersuchten Objekten an.

- Um die Arbeitslast zu optimieren, untersucht das Programm Dateien in einem bestimmten Format und einer bestimmten Größe. Die Liste der relevanten Formate und Größenbeschränkungen werden von Kaspersky-Experten festgelegt. Diese Liste wird mit den Antiviren-Datenbanken des Programms aktualisiert. Sie können auch Optimierungseinstellungen für Untersuchungen in der Programmoberfläche konfigurieren, z. B. für die Komponente Schutz vor bedrohlichen Dateien.

- Kaspersky Endpoint Security im Light Agent-Modus kommuniziert über einen KSN-Proxyserver mit KSN-Servern. Wird die direkte Interaktion mit KSN nicht unterstützt.

So aktivieren oder deaktivieren Sie Kaspersky Security Network

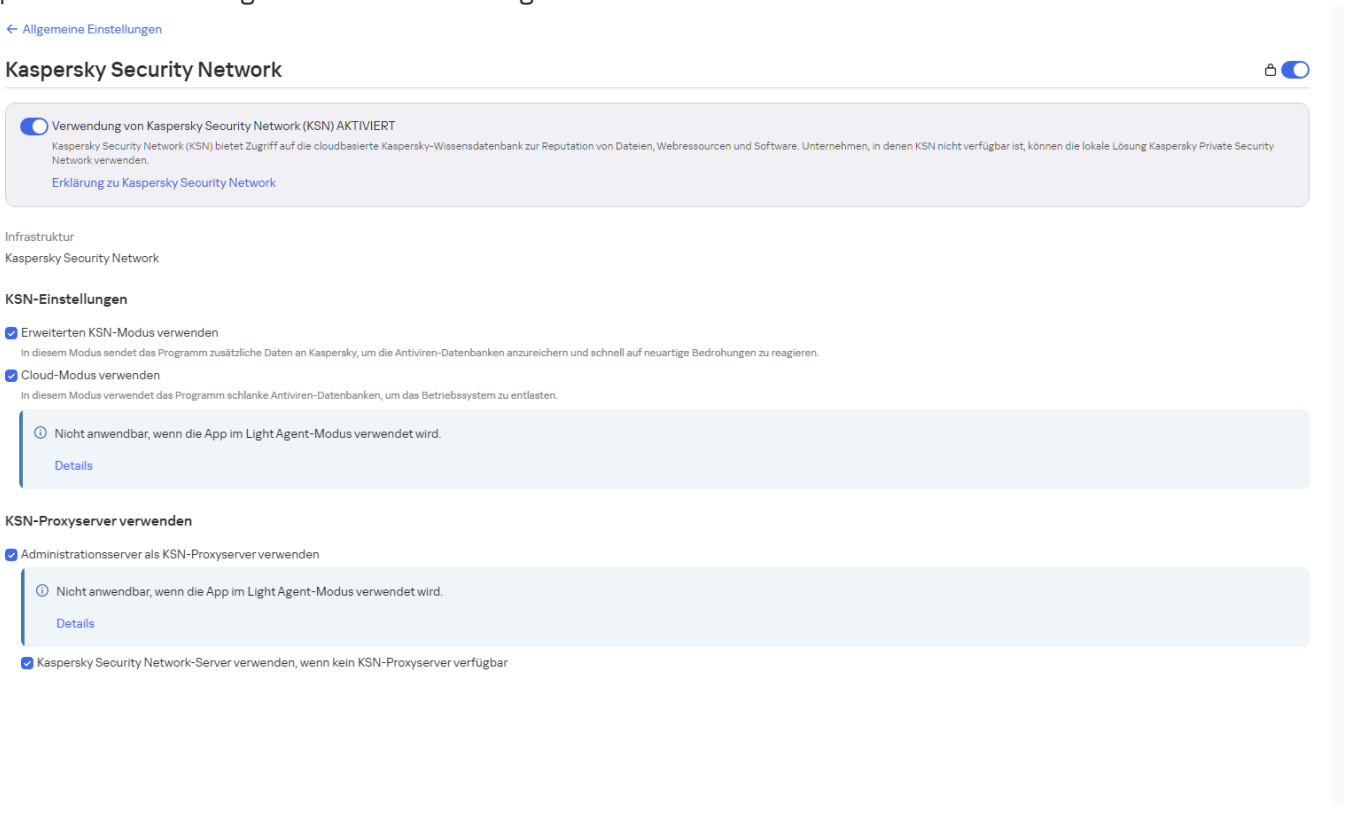
Kaspersky Endpoint Security verwendet standardmäßig den erweiterten KSN-Modus. Im *Erweiterten KSN-Modus* sendet Kaspersky Endpoint Security zusätzliche Daten an Kaspersky.

Es werden keine personenbezogenen Daten erhoben, verarbeitet oder gespeichert. Detaillierte Informationen über den Versand an Kaspersky, 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 Seite von Kaspersky. Die Datei mit dem Text der Erklärung zu Kaspersky Security Network ist im Lieferumfang der Anwendung enthalten.

So aktivieren oder deaktivieren Sie KSN in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Kaspersky Security Network**.
5. Verwenden Sie den Umschalter **Verwendung von Kaspersky Security Network (KSN)**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Wenn Sie die Verwendung von KSN aktiviert haben, wird das Fenster **Erklärung zu Kaspersky Security Network** geöffnet. Bitte lesen und akzeptieren Sie die Nutzungsbedingungen von Kaspersky Security Network (KSN), wenn Sie damit einverstanden sind.
7. Aktivieren oder deaktivieren Sie bei Bedarf das Kontrollkästchen **Erweiterten KSN-Modus verwenden**.
8. Speichern Sie die vorgenommenen Änderungen.



Kaspersky Security Network

So aktivieren oder deaktivieren Sie KSN über die Befehlszeile

1. Überprüfen Sie den Status von Kaspersky Security Network:

```
kesl-control --app-info
```

Das Programm zeigt den Status von KSN in der Zeile **Verwendung von Kaspersky Security Network** an:

- **Deaktiviert**
- **Standardmäßiger KSN-Modus**
- **Erweiterter KSN-Modus**.

2. Um den Standard-Modus von Kaspersky Security Network zu aktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings UseKSN=Basic --accept-ksn
```

3. Um den erweiterten KSN-Modus zu aktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings UseKSN=Extended --accept-ksn
```

4. Um Kaspersky Security Network zu deaktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings UseKSN=No
```

So aktivieren oder deaktivieren Sie die KSN-Nutzung (in der Programmoberfläche)

1. Öffnen Sie das Hauptfenster der App.
2. Klicken Sie im unteren Bereich des Programmhauptfensters auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im angezeigten Fenster eine der folgenden Optionen aus:
   - **Erweiterter KSN-Modus**, wenn Sie Kaspersky Security Network verwenden, Informationen aus der Wissensdatenbank abrufen und anonyme Statistikdaten sowie Informationen über die Typen und Quellen der Bedrohungen senden möchten.
   - **Standardmäßiger KSN-Modus**, wenn Sie Kaspersky Security Network verwenden und Informationen aus der Wissensdatenbank abrufen, aber keine anonymen Statistikdaten und Informationen über die Typen und Quellen der Bedrohungen senden möchten.
4. Klicken Sie auf die Schaltfläche **Aktivieren**.
5. Lesen Sie im Fenster **Verwendung von Kaspersky Security Network** die Erklärung zu Kaspersky Security Network aufmerksam durch und wählen Sie eine der folgenden Optionen aus:
   - **Ich bestätige, dass ich die Bedingungen der Erklärung zu Kaspersky Security Network vollständig gelesen habe, und sie verstehe und akzeptiere**.
   - **Ich lehne die Bedingungen der Erklärung zu Kaspersky Security Network ab**.
6. Klicken Sie auf die Schaltfläche **OK**.

Wenn die Verwendung des KSN aktiviert ist, verwendet Kaspersky Endpoint Security daher Informationen über die Reputation von Dateien, Webressourcen und Programmen, die vom Kaspersky Security Network empfangen werden.

Kaspersky Endpoint Security verwendet die folgenden Netzwerkeinstellungen für die Interaktion mit externen Diensten:

Adresse	Protokoll	Port
ds.kaspersky.com	HTTPS	443
ksn-a-stat-geo.kaspersky-labs.com	KSN	443, 1443
ksn-file-geo.kaspersky-labs.com	KSN	443, 1443
ksn-verdict-geo.kaspersky-labs.com	KSN	443, 1443
ksn-url-geo.kaspersky-labs.com	KSN	443, 1443
ksn-a-p2p-geo.kaspersky-labs.com	KSN	443, 1443
ksn-cinfo-geo.kaspersky-labs.com	KSN	443, 1443

Was ist der Cloud-Modus des Programms

Im *Cloud-Modus* verwendet Kaspersky Endpoint Security eine schlanke Version der Antiviren-Datenbanken, wodurch die Belastung des Arbeitsspeichers des Computers ungefähr halbiert wird.

Der Cloud-Modus kann nur verwendet werden, wenn Kaspersky Security Network aktiviert ist. Wenn Sie nicht an Kaspersky Security Network teilnehmen oder der Cloud-Modus deaktiviert ist, lädt Kaspersky Endpoint Security die komplette Version der Antiviren-Datenbanken von den Kaspersky-Servern herunter. Der Cloud-Modus ist standardmäßig aktiviert.

Wenn das Programm im Light Agent-Modus ausgeführt wird, ist der Cloud-Modus nicht verfügbar.

So aktivieren oder deaktivieren Sie den Cloud-Modus in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Kaspersky Security Network**.
5. Verwenden Sie den Schalter **Cloud-Modus verwenden**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie den Cloud-Modus über die Befehlszeile

1. Führen Sie den Befehl zum Anzeigen der allgemeinen Programmeinstellungen aus, um den aktuellen Status des Programms zu ermitteln:

   ```
   kesl-control --get-app-settings
   ```

   Das Programm zeigt seinen Status in der Zeile `CloudMode` an.

2. Um den Cloud-Modus zu aktivieren oder zu deaktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings CloudMode=<Yes|No>
```

Infolgedessen lädt Kaspersky Endpoint Security beim nächsten Update eine Light-Version oder Vollversion der Antiviren-Datenbanken herunter.

Falls die eingeschränkte Version der Antiviren-Datenbanken nicht verfügbar ist, schaltet Kaspersky Endpoint Security automatisch zur Verwendung der vollständigen Version der Antiviren-Datenbanken um.

Wozu dient der KSN-Proxy

Benutzercomputer, die vom Administrationsserver für Kaspersky Security Center verwaltet werden, können entweder direkt mit KSN interagieren oder über den KSN Proxy-Dienst.

Wenn das Programm im Light Agent-Modus ausgeführt wird, wird die direkte Kommunikation mit KSN nicht unterstützt. Kaspersky Endpoint Security interagiert über einen KSN-Proxyserver mit den KSN-Servern.

Der Dienst KSN Proxy bietet folgende Möglichkeiten:

- Der Computer des Benutzers kann Abfragen an KSN senden und Informationen an KSN übermitteln, auch ohne direkten Zugriff auf das Internet.
- Der KSN Proxy-Dienst übernimmt die Zwischenspeicherung von aufbereiteten Daten. Dadurch wird der Verbindungskanal zu dem externen Netzwerk entlastet und der Empfang angeforderter Informationen durch den Benutzercomputer wird beschleunigt.

Wenn KSN aktiviert ist und die KSN-Erklärung akzeptiert wurde, verwendet das Programm standardmäßig einen Proxyserver für die Verbindung mit Kaspersky Security Network. Als Proxyserver verwendet das Programm den Kaspersky Security Center-Administrationsserver über den TCP-Port 13111.

Sie können die Einstellungen des Proxy-Server-Dienstes von KSN in den Eigenschaften des Administrationsservers konfigurieren. Weitere Informationen zum KSN-Proxyserver finden Sie in der Hilfe zu Kaspersky Security Center.

Das Konfigurieren der Verbindungseinstellungen für den KSN-Proxyserver über die Befehlszeile ist nicht verfügbar.

KSN-Verbindung über einen Proxyserver in der Web Console konfigurieren

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Kaspersky Security Network**.
5. Verwenden Sie das Kontrollkästchen **Administrationsserver als KSN-Proxyserver verwenden**, um die Verwendung von KSN Proxy zu aktivieren oder zu deaktivieren.

6. Aktivieren oder deaktivieren Sie bei Bedarf das Kontrollkästchen **Kaspersky Security Network-Server verwenden, wenn kein KSN-Proxyserver verfügbar**. Dieses Kontrollkästchen ist standardmäßig aktiviert.

   Ist diese Option aktiviert, verwendet Kaspersky Endpoint Security die KSN-Server direkt, wenn der KSN Proxy-Service nicht verfügbar ist. Die KSN-Server können sich sowohl bei Kaspersky als auch bei Drittanbietern befinden (wenn Kaspersky Private Security Network verwendet wird).

7. Speichern Sie die vorgenommenen Änderungen.

Übertragung von Informationen an den Speicher von Kaspersky Security Center konfigurieren

In Kaspersky Security Center können Sie die Übertragung von Informationen über Dateien im Backup, Dateien in der Quarantäne, nicht verarbeitete Dateien und verbundene Geräte an den Speicher von Kaspersky Security Center aktivieren und deaktivieren.

So zeigen Sie Dateien in der Quarantäne auf Client-Geräten an

Die allgemeine Liste der Dateien, die von Kaspersky-Programmen auf Client-Geräten in die Quarantäne verschoben wurden, wird in Kaspersky Security Center gespeichert.

1. Wählen Sie im Hauptfenster der Web Console **Vorgänge** → **Datenverwaltung**.
2. Wechseln Sie zum Ordner **Quarantäne**.
3. Informationen zu Objekten in der Quarantäne werden im rechten Bereich der Konsole angezeigt.

So zeigen Sie Dateien im Backup auf Client-Geräten an

Die allgemeine Liste der Dateien, die von Kaspersky-Programmen auf Client-Geräten im Backup abgelegt wurden, wird in Kaspersky Security Center gespeichert.

1. Wählen Sie im Hauptfenster der Web Console **Vorgänge** → **Datenverwaltung**.
2. Wechseln Sie zum Ordner **Datei-Backups**.
3. Informationen zu Objekten, die im Backup abgelegt wurden, werden im rechten Bereich der Konsole angezeigt.

So zeigen Sie Informationen zu nicht verarbeiteten Dateien in der Liste der aktiven Bedrohungen an

1. Wählen Sie im Hauptfenster der Web Console **Vorgänge** → **Datenverwaltung**.
2. Wechseln Sie zum Ordner **Aktive Bedrohungen**.
3. Informationen zu nicht verarbeiteten Dateien in der Liste der aktiven Bedrohungen werden im rechten Bereich der Konsole angezeigt.

So zeigen Sie Informationen zu Hardware an, die mit Client-Geräten verbunden ist

1. Wählen Sie im Hauptfenster der Web Console **Vorgänge** → **Datenverwaltung**.
2. Wechseln Sie zum Ordner **Hardware**.
3. Informationen zu Geräten werden im rechten Bereich der Konsole angezeigt.

Informationen werden übertragen, wenn die Komponente Gerätekontrolle aktiviert ist.

So zeigen Sie Informationen zu Programmen auf Client-Geräten an

1. Wählen Sie im Hauptfenster der Web Console **Vorgänge** → **Drittanbieter-Programme**.
2. Wechseln Sie zum Ordner **Programm-Registry**.
3. Informationen zu Programmen werden im rechten Bereich der Konsole angezeigt.

Die Informationen werden übertragen, wenn die Komponente Programmkontrolle aktiviert ist.

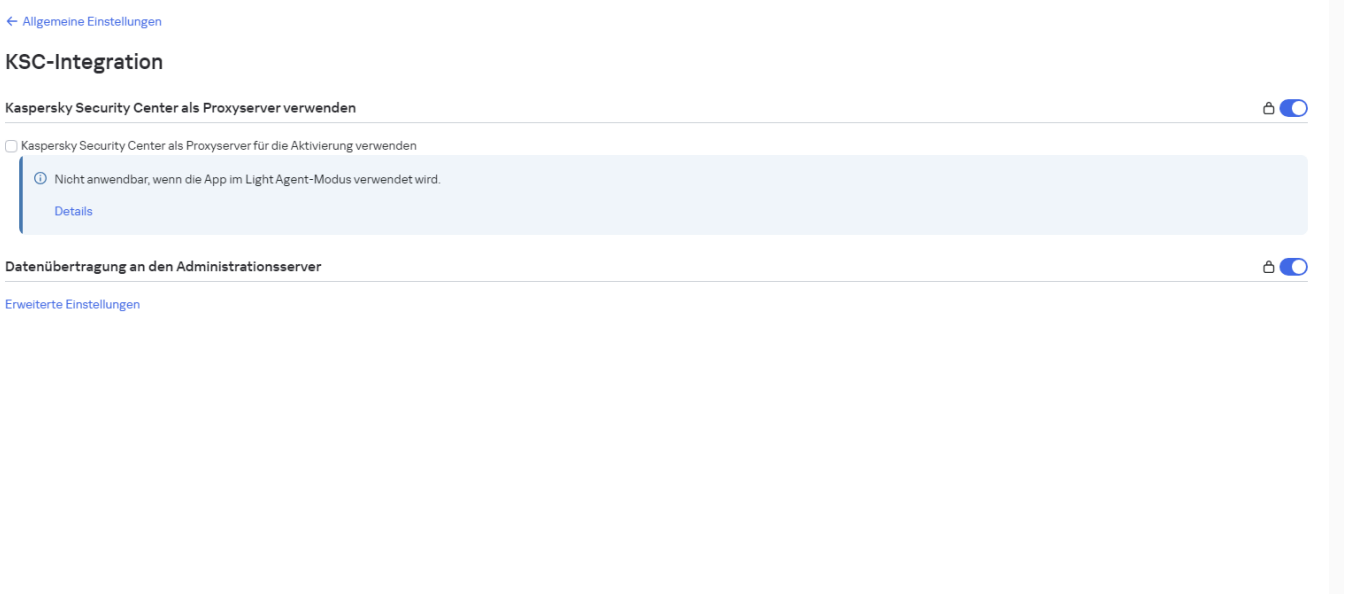
So konfigurieren Sie die Integration mit dem Administrationsserver

Gehen Sie wie folgt vor, um die Integration mit dem Administrationsserver in den Eigenschaften der Richtlinie zu konfigurieren:

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **KSC-Integration**.
5. Klicken Sie auf den Link **Zusätzliche Einstellungen**.
6. Wählen Sie die Kategorien von Ereignissen auf Client-Computern aus, deren Informationen an den Administrationsserver weitergeleitet werden müssen:
   - **Über Dateien in der Quarantäne** Dieses Kontrollkästchen aktiviert oder deaktiviert die Übertragung von Informationen über in die Quarantäne verschobene Dateien an den Administrationsserver.
   - **Informationen zu Dateien im Backup**. Das Kontrollkästchen aktiviert oder deaktiviert die Übertragung von Informationen über Dateien im Backup an den Administrationsserver.
   - **Informationen zu nicht verarbeiteten Dateien**. Dieses Kontrollkästchen aktiviert und deaktiviert das Senden von Benachrichtigungen über Dateien, die während der Untersuchung nicht verarbeiteten wurden, an den Administrationsserver.
   - **Informationen zu installierten Geräten**. Dieses Kontrollkästchen aktiviert oder deaktiviert die Übertragung von Informationen über die auf dem verwalteten Client-Gerät installierten Geräte an den Administrationsserver.
   - **Informationen zu gestarteten Programmen**. Das Kontrollkästchen aktiviert oder deaktiviert die Übertragung der Liste mit den Anwendungen, die durch die Inventarisierungsaufgabe auf dem Client-Gerät erkannt wurden, an den Administrationsserver.
7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Gehen Sie wie folgt vor, um die Integration mit dem Administrationsserver in den Eigenschaften eines verwalteten Geräts zu konfigurieren:

1. Wählen Sie im Hauptfenster der Web Console **Asset-Management** → **Assets (Geräte)** → **Verwaltete Geräte**.
2. Klicken Sie auf den Link **<Gerätename>**.
3. Wählen Sie die Registerkarte **Programme** aus und klicken Sie auf den Link **Kaspersky Endpoint Security**.
4. Wechseln Sie auf der Registerkarte **Programmeinstellungen** zum Abschnitt **Speichereinstellungen**.
5. Klicken Sie unter **Einstellungen für die Datenübertragung an den Administrationsserver** auf die Schaltfläche **Konfigurieren**.
6. Im Fenster **Einstellungen für die Datenübertragung** können Sie das Senden von Informationen an den Administrationsserver aktivieren oder deaktivieren:
   - **Über Dateien im Backup informieren**. Das Kontrollkästchen aktiviert oder deaktiviert die Übertragung von Informationen über Dateien im Backup an den Administrationsserver.
   - **Über Dateien in der Quarantäne informieren**. Das Kontrollkästchen aktiviert oder deaktiviert die Übertragung von Informationen über unter Quarantäne gestellte Dateien an den Administrationsserver.
   - **Über nicht verarbeitete Dateien informieren**. Dieses Kontrollkästchen aktiviert und deaktiviert das Senden von Benachrichtigungen über Dateien, die während der Untersuchung nicht verarbeiteten wurden, an den Administrationsserver.
   - **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.
   - **Über auf dem Gerät gefundene Programme informieren**. Das Kontrollkästchen aktiviert oder deaktiviert die Übertragung der Liste mit den Anwendungen, die durch die Inventarisierungsaufgabe auf dem Client-Gerät erkannt wurden, an den Administrationsserver.
7. Speichern Sie die vorgenommenen Änderungen.



So konfigurieren Sie den Programmstart

Programmstart konfigurieren

Sie können die maximale Anzahl fehlgeschlagener Startversuche und das Start-Timeout für Kaspersky Endpoint Security anpassen. Dadurch kann das System entlastet werden, wenn das Programm über längere Zeit nicht gestartet werden kann. Standardmäßig beträgt die maximale Anzahl erfolgloser aufeinanderfolgender Versuche zum Starten des Programms 5 und das maximale Timeout 3 Minuten.

So konfigurieren Sie den Programmstart in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Interaktion mit dem Benutzer**.
5. Geben Sie unter **Einstellungen für den Programmstart** Werte in die folgenden Felder ein:
   - **Maximale Anzahl an fehlgeschlagenen Versuchen, das Programm zu starten**. Standardwert: 5.
   - **Maximale Wartezeit für den Programmstart (Min.)**. Standardwert: 3.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie den Programmstart über die Befehlszeile

In der Befehlszeile können Sie die Einstellungen für den Programmstart 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 Anwendung festlegen. Der Parameter kann die Werte 1 bis 10 annehmen. Standardwert: 5.

Mit dem Parameter `StartupTimeout` können Sie die maximale Wartezeit für den Programmstart (in Minuten) festlegen, nach deren Ablauf der Prozess kesl neu gestartet wird. Der Parameter kann die Werte 1 bis 60 annehmen. Standardwert: 3.

Kritische Updates anwenden

Sie können das Programm so konfigurieren, dass es beim Empfang kritischer Updates automatisch neu gestartet wird. Standardmäßig wird das Programm automatisch neu gestartet, wenn innerhalb von 24 Stunden nach der Installation des Programms beim ersten Update der Datenbanken und Module kritische Updates empfangen werden.

So konfigurieren Sie den automatischen Programmneustart in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Interaktion mit dem Benutzer**.
5. Aktivieren Sie im Block **Anwenden von wichtigen Updates** das Kontrollkästchen **Anwendung automatisch neu starten, wenn wichtige Updates empfangen werden**.

   Kaspersky Endpoint Security wird automatisch neu gestartet, wenn kritische Updates empfangen werden.
6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den automatischen Programmneustart über die Befehlszeile

Über die Befehlszeile können Sie den automatischen Programmneustart mithilfe des Parameters `UrgentUpdateRestartEnabled` in den allgemeinen Programmeinstellungen konfigurieren.

Um das Programm bei der Installation kritischer Updates automatisch neu zu starten, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings UrgentUpdateRestartEnabled=Yes
```

Berechtigungen für die Aufgabenverwaltung konfigurieren

In Kaspersky Security Center können Sie die folgenden Berechtigungen für Benutzer konfigurieren:

- Berechtigung zur Verwendung von lokalen Aufgaben, die in Kaspersky Endpoint Security erstellt wurden. Wenn die Kaspersky Security Center-Richtlinie Benutzer daran hindert, lokale Aufgaben anzuzeigen, zu bearbeiten, zu erstellen und zu löschen, sind Informationen zu den Aufgaben Scan_My_Computer, Critical_Areas_Scan, Container_Scan, Inventory_Scan, Update (im Standard-Modus) und Rollback (im Standard-Modus) nicht verfügbar.
- Berechtigung zum Anzeigen und Verwalten von Aufgaben auf Client-Geräten, die in Kaspersky Security Center erstellt wurden.

So konfigurieren Sie die Berechtigungen für die Aufgabenverwaltung in der Web Console:

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Interaktion mit dem Benutzer**.
5. Wählen Sie unter **Zulässige Aktionen** die Aktionen aus, die Benutzer auf ihren Geräten ausführen dürfen:

   - **Auf lokale Aufgaben zugreifen**. Wenn das Kontrollkästchen aktiviert ist, werden die lokalen Aufgaben auf der lokalen Programmoberfläche von Kaspersky Endpoint Security angezeigt. Wenn weitere Einschränkungen der Richtlinie dies nicht verhindern, können Benutzer verfügbare lokale Aufgaben in der grafischen Benutzeroberfläche des Programms oder über die Befehlszeile konfigurieren, ausführen, erstellen und löschen.

   - **Gruppenaufgaben verwalten**. Wenn dieses Kontrollkästchen aktiviert ist, können Benutzer die in Kaspersky Security Center konfigurierten Gruppenaufgaben auf den Client-Geräten verwalten. Aufgaben können über die grafische Benutzeroberfläche des Programms oder über die Befehlszeile ausgeführt werden.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Kennwortschutz

Mit dem Kennwortschutz können Sie den Benutzerzugriff auf Änderungen an Kaspersky Endpoint Security entsprechend den gewährten Berechtigungen beschränken (z. B. die Berechtigung zum Anzeigen von Programmberichten). Durch die Beschränkung des Zugriffs auf die Programmeinstellungen wird das Risiko unbefugter oder unbeabsichtigter Änderungen am Programm verringert.

Funktionsweise des Kennwortschutzes

1. **Ein Benutzer versucht, eine von der Komponente kontrollierte Aktion auszuführen**

   Zum Beispiel das Deaktivieren von Schutzkomponenten oder das Anzeigen von Berichten von Kaspersky Endpoint Security.
2. **Kaspersky Endpoint Security überprüft die Benutzerrechte**

   Wenn der Benutzer über die entsprechende Berechtigung verfügt, wird die Aktion erfolgreich ausgeführt. Wenn der Benutzer nicht über die entsprechende Berechtigung verfügt, blockiert das Programm die Aktion und zeigt einen Fehler an.

   In der grafischen Benutzeroberfläche von Kaspersky Endpoint Security können verbotene Aktionen nicht angezeigt oder bearbeitet werden.

Kennwortschutz konfigurieren

1 Kennwortschutz aktivieren

Der Kennwortschutz ist standardmäßig deaktiviert. Aktivieren Sie die Komponente in der Web Console, in der Verwaltungskonsole oder in der Befehlszeile mit folgendem Befehl:

```
kesl-control --set-permission-manager-settings Enabled=Yes
```

2 Benutzerberechtigungen konfigurieren

Standardmäßig sind im Programm Benutzerberechtigungen für vordefinierte Benutzergruppen konfiguriert: *kesladmin*, *kesluser*, *keslaudit*.

Konfigurieren Sie die Benutzerberechtigungen für diese Gruppen oder erstellen Sie einen neuen Benutzer oder eine neue Benutzergruppe.

> Damit das Programm korrekt funktioniert, wird empfohlen, die Berechtigungen für mindestens eine Gruppe anzupassen.

So konfigurieren Sie benutzerdefinierte Berechtigungen in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Selbstschutz**.
5. Stellen Sie sicher, dass sich der Kippschalter für die Komponente in der Position **Kennwortschutz AKTIVIERT** befindet.
6. Klicken Sie auf den Link **Benutzerberechtigungen**.

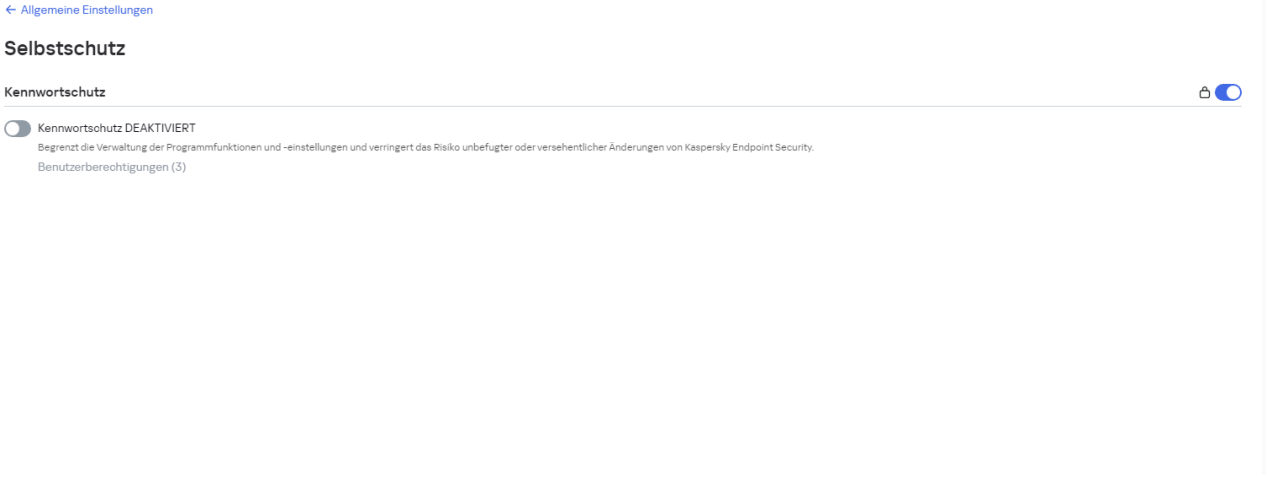
   Dadurch wird ein Fenster mit Benutzern und deren Berechtigungen geöffnet.
7. Wenn Sie die Berechtigungen für vordefinierte Gruppen ändern möchten, klicken Sie auf den Namen der Gruppe.

   Wenn Sie die Berechtigungen für einen anderen Benutzer oder eine andere Gruppe ändern möchten:

   a. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   b. Wählen Sie einen Benutzer oder eine Gruppe aus Active Directory aus oder geben Sie den Namen manuell ein.
8. Aktivieren Sie die Kontrollkästchen neben den Berechtigungen, die Sie dem Benutzer oder der Gruppe gewähren möchten.

9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Selbstschutz

So konfigurieren Sie benutzerdefinierte Berechtigungen in der Befehlszeile

1. Um die Liste der aktuellen Einstellungen für den Kennwortschutz anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-permission-manager-settings
```

2. Um die Berechtigungen eines Benutzers oder einer Gruppe zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-permissions <principal> [--group] <permissions>=<Yes|No> [--file <file name>] [--
json]
```

3. Um einen Benutzer oder eine Gruppe, für den bzw. die Berechtigungen konfiguriert wurden, zu entfernen, führen Sie den folgenden Befehl aus:

```
kesl-control --remove-permissions <principal> [--group]
```

Symbole

Befehlsoptionen

Parameter	Description
`--group`	Die Einstellung gilt für eine Gruppe. Wenn die Option `--group` nicht angegeben ist, gilt die Einstellung für einen einzelnen Benutzer.
`--file <file name>`	Ausgeben von Parametern in eine Datei oder Importieren von Parametern aus einer Datei. Geben Sie einen `<file name>` ein.
`--json`	Ausgeben von Parametern in eine JSON-Datei oder Importieren von Parametern aus einer JSON-Datei. Diese Option kann nur angegeben werden, wenn die Option `--file <file name>` angegeben ist.
`principal`	Name des Benutzers oder der Benutzergruppe.

Parameter	Description
`permissions`	Benutzerdefinierte Berechtigungen. Geben Sie `Yes` an, um dem Benutzer eine Aktion zu erlauben, oder `No`, um sie zu verweigern. • `StopProtection`. Deaktivieren von Schutzkomponenten. • `StopSecurityControl`. Überwachungskomponenten deaktivieren • `StartProtection`. Aktivieren von Schutzkomponenten. • `StartSecurityControl`. Aktivieren von Kontrollkomponenten • `ApplicationSettings`. Konfigurieren des Programms • `ViewReports`. Berichte anzeigen • `RestoreFromBackup`. Wiederherstellen aus dem Backup • `RemoveLicenseKey`. Schlüssel löschen • `AddLicense`. Hinzufügen eines Schlüssels • `DisablePolicy`. Deaktivieren der Richtlinie für Kaspersky Security Center

Beispiele

Berechtigung zum Anzeigen von Berichten für die Gruppe *kesluser* widerrufen:

```
kesl-control --set-permissions kesluser --group ViewReports=No
```

Verwaltung von Kontrollkomponenten für *new-user* erlauben:

```
kesl-control --set-permissions new-user startSecurityControl=Yes StopSecurityControl=Yes
```

Besonderheiten beim Kennwortschutz

- Wenn der Kennwortschutz deaktiviert ist, wird anhand von Benutzerrollen festgelegt, ob ein Benutzer das Programm verwalten darf.
- Wenn die Zugriffsebene eines Benutzers sowohl durch Gruppenberechtigungen als auch durch individuelle Berechtigungen geregelt wird, setzen individuelle Berechtigungen die Gruppenberechtigungen außer Kraft. Das heißt, selbst wenn die individuellen Berechtigungen eines Benutzers restriktiver sind als die Gruppenberechtigungen desselben Benutzers, gelten die restriktiveren Berechtigungen.

  Wenn beispielsweise die Verwaltung des Programms für die Gruppe *kesluser* verboten ist, können Sie die Verwaltung des Programms dennoch einem einzelnen Benutzer erlauben, der Mitglied dieser Gruppe ist. Ein solcher Benutzer darf das Programm weiterhin verwalten, obwohl die Gruppenberechtigungen dies nicht erlauben.
- Wenn der Kennwortschutz aktiviert ist und ein Benutzer weder über individuelle noch über Gruppenberechtigungen verfügt, sind alle Aktionen verboten.

Über benutzerdefinierte Berechtigungen

Wenn der Kennwortschutz aktiviert ist, wird der Zugriff auf die Verwaltung von Kaspersky Endpoint Security mithilfe von *Benutzerberechtigungen* gesteuert. Benutzerberechtigungen legen die Rechte eines Benutzers fest (siehe Tabelle unten).

Erlaubnis	Berechtigungen
Konfigurieren des Programms	Anzeigen und Bearbeiten der Programmeinstellungen. Verwalten der Aufgabeneinstellungen in der grafischen Oberfläche der Anwendung und über die Befehlszeile, ohne den Befehl `sudo` zu verwenden. beliebigen Benutzern beliebige Rollen zuweisen beliebigen Benutzern beliebige Rollen entziehen (der Administrator kann sich die Rolle admin nicht selbst entziehen) Verwalten der Aufgabe *Rollback des Datenbanken-Updates*. Verwalten von Komponenten: • Managed Detection and Response • Endpoint Detection and Response Optimum
Aktivieren von Schutzkomponenten. Schutzkomponenten deaktivieren	Verwalten von Komponenten: • Komponente "Schutz vor bedrohlichen Dateien". • Untersuchung von Wechseldatenträgern • Verhaltensanalyse • Schutz vor Verschlüsselung • Schutz vor modifizierten USB-Geräten • Schutz vor E-Mail-Bedrohungen • Schutz vor Web-Bedrohungen • Schutz vor Netzwerkbedrohungen • Firewall-Verwaltung • Überwachung der System-Integrität • Ausführungsprävention für Objekte (EDR Optimum) (*EDRO_Prevention*) • Endpoint Detection and Response Expert (On-Premises) • Endpoint Detection and Response Expert (cloud) • Network Detection and Response (KATA) • Sandbox • Integration mit KUMA
Aktivieren von Kontrollkomponenten Überwachungskomponenten deaktivieren	Verwalten von Komponenten: • Gerätekontrolle • Programmkontrolle • Web-Kontrolle
Berichte anzeigen	Anzeigen von Aufgabenberichten Ereignisse anzeigen
Wiederherstellen aus dem Backup	Speicher der Benutzer anzeigen und verwalten
Löschen des Schlüssels Schlüssel hinzufügen	Verwaltung der Lizenzierung der App
Deaktivieren der Richtlinie für Kaspersky Security Center	Deaktivieren oder Aktivieren der Kaspersky Security Center-Richtlinie auf dem Gerät.

Besonderheiten bei benutzerdefinierten Berechtigungen

- Benutzerberechtigungen haben keinen Einfluss auf das Anzeigen der Aufgabenliste, das Anzeigen von Objekten im Backup sowie das Anzeigen der Einstellungen und des Status des Programms.

  Alle Benutzer dürfen die folgenden Aufgaben verwalten:

  - Untersuchungsaufgaben (*Benutzerdefinierte Untersuchung*, *Untersuchung von Containern*, *Benutzerdefinierte Untersuchung von Containern*, *Untersuchung wichtiger Bereiche*, *Schadsoftware-Untersuchung*)
  - *Inventarisierung*
  - *Update der Datenbanken und Programm-Module*

- *Überwachung der System-Integrität*
- *IOC-Suche*

- Sie können den Hauptlizenzschlüssel nicht in der grafischen Oberfläche hinzufügen oder entfernen, wenn das Gerät durch eine Kaspersky Security Center-Richtlinie gesteuert wird. Ein Benutzer mit den Berechtigungen *Schlüssel hinzufügen* und *Schlüssel löschen* kann einen Reserveschlüssel hinzufügen oder einen Lizenzschlüssel zur Aktivierung anderer Kaspersky-Lösungen (Add-on) hinzufügen.

  Wenn das Gerät nicht durch eine Richtlinie verwaltet wird, kann der Benutzer den Hauptlizenzschlüssel entfernen oder hinzufügen.

Standardmäßige Benutzerberechtigungen

Standardmäßig sind im Programm Benutzerberechtigungen für vordefinierte Benutzergruppen konfiguriert: *kesladmin*, *kesluser*, *keslaudit*. Für Benutzer, die nicht Mitglied dieser Gruppen sind, sind alle Vorgänge mit dem Programm untersagt.

Benutzerberechtigungen vordefinierter Gruppen

Erlaubnis	kesladmin	kesluser	keslaudit
Konfigurieren des Programms	✓	–	–
Aktivieren von Schutzkomponenten.	✓	–	–
Schutzkomponenten deaktivieren	✓	–	–
Aktivieren von Kontrollkomponenten	✓	–	–
Überwachungskomponenten deaktivieren	✓	–	–
Berichte anzeigen	✓	–	✓
Wiederherstellen aus dem Backup	✓	–	–
Löschen des Schlüssels	✓	–	–
Schlüssel hinzufügen	✓	–	–
Deaktivieren der Richtlinie für Kaspersky Security Center	✓	–	–

Leistungseinstellungen

Die Untersuchung des Computers mithilfe von Kaspersky Endpoint Security kann erhebliche Systemressourcen in Anspruch nehmen. Zur Optimierung der Systemlast stehen Ihnen folgende Möglichkeiten zur Verfügung:

- Geplante Aufgaben bei Akkubetrieb aufschieben oder überspringen
- Prozessorauslastung für Untersuchungsaufgaben begrenzen (%)
- Nutzung des residenten Speichers durch die Anwendung begrenzen
- Speicher einiger Prozesse von der Untersuchung ausschließen

Geplante Aufgaben bei Akkubetrieb aufschieben oder überspringen

Wenn Ihr Gerät im Akkubetrieb läuft und Sie die Ressourcennutzung durch Kaspersky Endpoint Security reduzieren möchten, können Sie geplante Aufgaben überspringen:

- Alle Untersuchungsaufgaben (Benutzerdefinierte Untersuchung, Untersuchung von Containern, Benutzerdefinierte Untersuchung von Containern, Untersuchung wichtiger Bereiche, *Schadsoftware-Untersuchung*)
- *Inventar*
- *Update der Datenbanken und Programm-Module*
- *Prüfung der Anwendungsintegrität*
- *IOC-Untersuchung*

Bei Bedarf können Sie die erforderlichen Aufgaben manuell ausführen.

Geplante Aufgaben im Akkubetrieb in der Web Console abbrechen

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Leistung**.
5. Aktivieren Sie die Funktion **Geplante Aufgaben bei Akkubetrieb aufschieben oder überspringen**.
   Kaspersky Endpoint Security *bricht* geplante Aufgaben ab.
6. Speichern Sie die vorgenommenen Änderungen.

Geplante Aufgaben im Akkubetrieb über die Befehlszeile abbrechen

Über die Befehlszeile können Sie das Abbrechen geplanter Aufgabenausführungen mithilfe des Parameters `PowerSaveMode` in den allgemeinen Einstellungen der Anwendung konfigurieren.

Um geplante Aufgaben abzubrechen, wenn das Gerät im Akkubetrieb läuft, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings PowerSaveMode=Yes
```

Prozessorauslastung für Untersuchungsaufgaben begrenzen (%)

Sie können die CPU- und Arbeitsspeichernutzung für die Aufgaben *Schadsoftware-Untersuchung*, *Untersuchung wichtiger Bereiche*, *Inventarisierung* und *Untersuchung von Containern* begrenzen (der ODS-, ContainerScan- und InventoryScan-Typen). Standardmäßig ist der Grenzwert für die Arbeitsspeichernutzung auf 8192 MB festgelegt. Für die CPU-Auslastung ist kein Grenzwert festgelegt.

Es wird empfohlen, den Grenzwert für die Arbeitsspeichernutzung für Untersuchungsaufgaben unter dem Grenzwert für die Nutzung des residenten Speichers festzulegen, damit Untersuchungsaufgaben nicht den gesamten verfügbaren Arbeitsspeicher belegen und einen Neustart des Programms verursachen.

Beachten Sie, dass die kombinierte Kapazität aller CPU-Kerne als 100 % betrachtet wird.

Das Tool `top` zeigt die Prozessorauslastung an und geht dabei davon aus, dass die Ressource eines Kerns 100% beträgt. Ein Wert von 400% bedeutet daher für eine Prozessor mit 10 Kernen (insgesamt 1000% laut Tool `top`), dass der gesamte Prozessor (alle Kerne in Summe) zu 40% ausgelastet ist. Wenn Sie möchten, dass der Wert in der Ausgabe des Dienstprogramms `top` auf denselben 10 Kernen nie 150 % überschreitet, legen Sie als Grenzwert für die CPU-Auslastung `15%` fest.

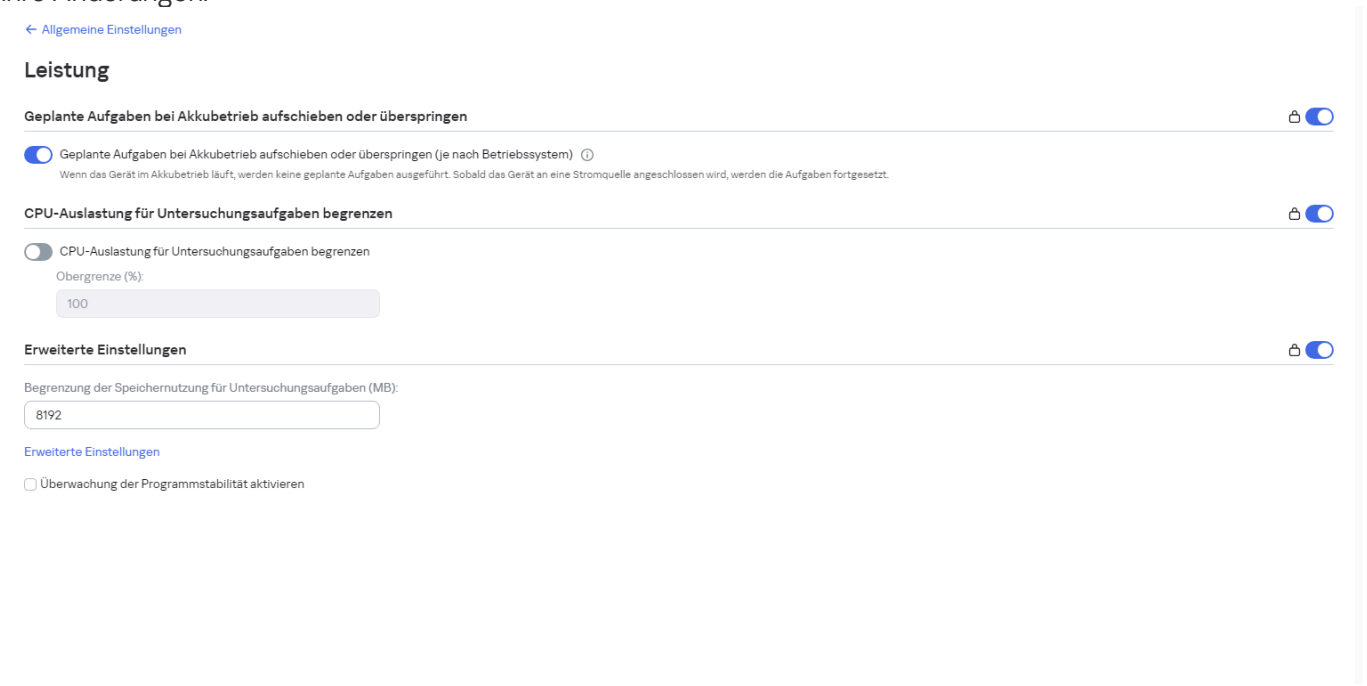
Der Grenzwert für die CPU-Auslastung wird auf die Aufgaben *Schadsoftware-Untersuchung*, *Untersuchung wichtiger Bereiche*, *Inventarisierung* und *Untersuchung von Containern* angewendet. Das bedeutet, dass die CPU-Auslastung den konfigurierten Wert überschreiten kann.

Die Begrenzung der CPU-Auslastung ist auf Geräten mit CentOS 5.2 und 5.4 nicht möglich.

So begrenzen Sie die Nutzung von Arbeitsspeicher- und CPU-Ressourcen in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Leistung**.
5. Aktivieren Sie die Funktion **CPU-Auslastung für Untersuchungsaufgaben begrenzen**.
6. Geben Sie im Feld **Obergrenze (%)** die maximale Auslastung aller CPU-Kerne an. Der Wert muss eine ganze Zahl von 10 bis 100 sein.
7. Geben Sie unter **Erweiterte Einstellungen** im entsprechenden Feld den Grenzwert für die Arbeitsspeichernutzung für Untersuchungsaufgaben (MB) an. Standardwert: 8192.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Leistung

So begrenzen Sie die Nutzung von Arbeitsspeicher- und CPU-Ressourcen über die Befehlszeile

In der Befehlszeile können Sie mithilfe der Einstellungen `UseOnDemandCPULimit` und `OnDemandCPULimit` in den allgemeinen Programmeinstellungen einen Grenzwert für die Nutzung von CPU-Ressourcen durch Untersuchungsaufgaben anpassen.

1. Aktivieren Sie die CPU-Begrenzung für Untersuchungsaufgaben, indem Sie den folgenden Befehl ausführen:

   ```
   kesl-control --set-app-settings UseOnDemandCPULimit = Yes
   ```

2. Legen Sie einen CPU-Grenzwert fest, indem Sie den folgenden Befehl ausführen:

   ```
   kesl-control --set-app-settings OnDemandCPULimit =<value>
   ```

   Der Grenzwert wird in Prozent angegeben. Mögliche Werte sind ganze Zahlen von 10 bis 100.

3. Geben Sie den Grenzwert für die Arbeitsspeichernutzung für Untersuchungsaufgaben an, indem Sie die Einstellung `ScanMemoryLimit` in der Konfigurationsdatei kesl.ini verwalten.

Nutzung des residenten Speichers durch die Anwendung begrenzen

Sie können die Nutzung des residenten Speichers durch die Anwendung begrenzen. Standardmäßig ist der Grenzwert auf bis zu 50 % des Arbeitsspeichers festgelegt, jedoch mindestens 2 GB und höchstens 16 GB.

So begrenzen Sie die Nutzung des residenten Speichers in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Leistung**.
5. Klicken Sie unter **Erweiterte Einstellungen** auf den Link **Erweiterte Einstellungen** und aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Speichernutzung des Programms begrenzen**.

   In der Dropdown-Liste können Sie auswählen, auf welche Weise die Verwendung des residenten Speichers begrenzt werden soll:

   - **Exakten Wert angeben (%)**. Wenn diese Option ausgewählt ist, wird das Feld **Exakter Wert (%)** verfügbar, in dem Sie einen Prozentwert angeben können. Der Standardwert ist 50%
   - **Exakten Wert angeben (MB)**. Wenn diese Option ausgewählt ist, wird das Feld **Exakter Wert (MB)** verfügbar, in dem Sie einen Wert in Megabyte angeben können. Standardmäßig ist ein Wert von 2000 MB festgelegt.
   - **Größeren der beiden Werte anwenden (% oder MB)**. Wenn diese Option ausgewählt ist, werden die Felder **Exakter Wert (%)** und **Exakter Wert (MB)** verfügbar, in denen Sie die erforderlichen Werte angeben können.
   - **Kleineren der beiden Werte anwenden (% oder MB)**. Wenn diese Option ausgewählt ist, werden die Felder **Exakter Wert (%)** und **Exakter Wert (MB)** verfügbar, in denen Sie die erforderlichen Werte angeben können.
   - **Automatisch begrenzen (empfohlen)**. Wenn Sie diese Option auswählen, wird die Verwendung des residenten Speichers automatisch begrenzt (Standardwert).
6. Speichern Sie die vorgenommenen Änderungen.

Um die Änderungen zu übernehmen, starten Sie Kaspersky Endpoint Security auf dem verwalteten Gerät neu, nachdem die Richtlinie übernommen wurde.

So begrenzen Sie die Nutzung des residenten Speichers über die Befehlszeile

Sie können die Einstellung `MaxMemory` nicht über die Befehlszeile verwalten. Verwenden Sie die Konfigurationsdatei kesl.ini, um den Grenzwert für den residenten Speicher zu konfigurieren.

Es wird empfohlen, die Änderung der Standardwerte unter Anleitung von Spezialisten des Technischen Supports vorzunehmen.

Der Parameter `MaxMemory` kann folgende Werte annehmen:

- `off` – Die Nutzung des residenten Speichers ist nicht beschränkt.
- `<value>%` – ein Wert zwischen 1 und 100 Prozent des Arbeitsspeichers.

- `<value>MB` – ein Wert in Megabyte.
- `lowest/<value>%/<value>MB` – der kleinere Wert aus Prozentwert und absolutem Wert in Megabyte.
- `highest/<value>%/<value>MB` – der größere Wert aus Prozentwert und absolutem Wert in Megabyte.
- `auto` (Standard) – automatischer Grenzwert.

Ausschließen des Prozessspeichers von Untersuchungen

Sie können den Speicher ausgewählter Prozesse von der Untersuchung ausschließen.

Speicher von Prozessen in der Web Console von der Untersuchung ausschließen

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Leistung**.
5. Klicken Sie im Block **Erweiterte Einstellungen** auf den Link **Ausnahmen für die Untersuchung des Prozess-Speichers konfigurieren**.
6. Daraufhin wird ein Fenster geöffnet. Klicken Sie in diesem Fenster auf die Schaltfläche **Hinzufügen** und geben Sie den Pfad zur ausführbaren Datei des Prozesses an.
   Pfadanforderungen:
7. Muss mit `/` beginnen (absoluter Pfad)
   a. Darf keine verbotenen Zeichen enthalten:
      - `\0` (Nullbyte): durch das Betriebssystem verboten.
      - Schrägstrich (`/`) innerhalb eines Datei- oder Verzeichnisnamens: wird als Trennzeichen verwendet.
8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Speicher von Prozessen über die Befehlszeile von der Untersuchung ausschließen

Über die Befehlszeile können Sie Untersuchungsausschlüsse für den Prozess-Speicher mithilfe des Parameters `MemScanExcludedProgramPath.item_#` in den allgemeinen Anwendungseinstellungen konfigurieren.

Sie können den Wert der Einstellung mithilfe von Befehlszeilenschaltern oder einer Konfigurationsdatei ändern, die alle allgemeinen Programmeinstellungen enthält.

Der Parameter `MemScanExcludedProgramPath.item_#` enthält den vollständigen Pfad zum Prozess im lokalen Verzeichnis. Bei der Angabe des Pfades können Masken verwendet werden.

Sie können mehrere Prozesse angeben, die von der Untersuchung ausgeschlossen werden sollen.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Optimierung der Ressourcenauslastung durch die Anwendung

Netzwerkeinstellungen

Sie können den Proxyserver für die Internetverbindung konfigurieren, den Überwachungsmodus für Netzwerkports auswählen und die Untersuchung geschützter Verbindungen einrichten.

So verwalten Sie die Proxy-Einstellungen

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 Proxyserver für folgende Vorgänge verwenden: für den Zugriff auf die Aktivierungsserver von Kaspersky, auf die Update-Quellen für Datenbanken und Module der Anwendung und auf Kaspersky Security Network sowie für die Untersuchung von Website-Zertifikaten mit dem Schutz vor Web-Bedrohungen.

Standardmäßig ist die Verwendung eines Proxyservers deaktiviert.

Wenn Sie Geräte aktivieren, die sich in einem isolierten Netzwerksegment ohne Internetzugriff befinden, können Sie anhand eines Aktivierungscodes den Kaspersky Security Center Administrationsserver als Proxyserver für den Zugriff auf die Aktivierungsserver von Kaspersky verwenden.

So konfigurieren Sie die Verwendung von Kaspersky Security Center als Proxyserver zur Aktivierung des Programms in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Geräteverwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

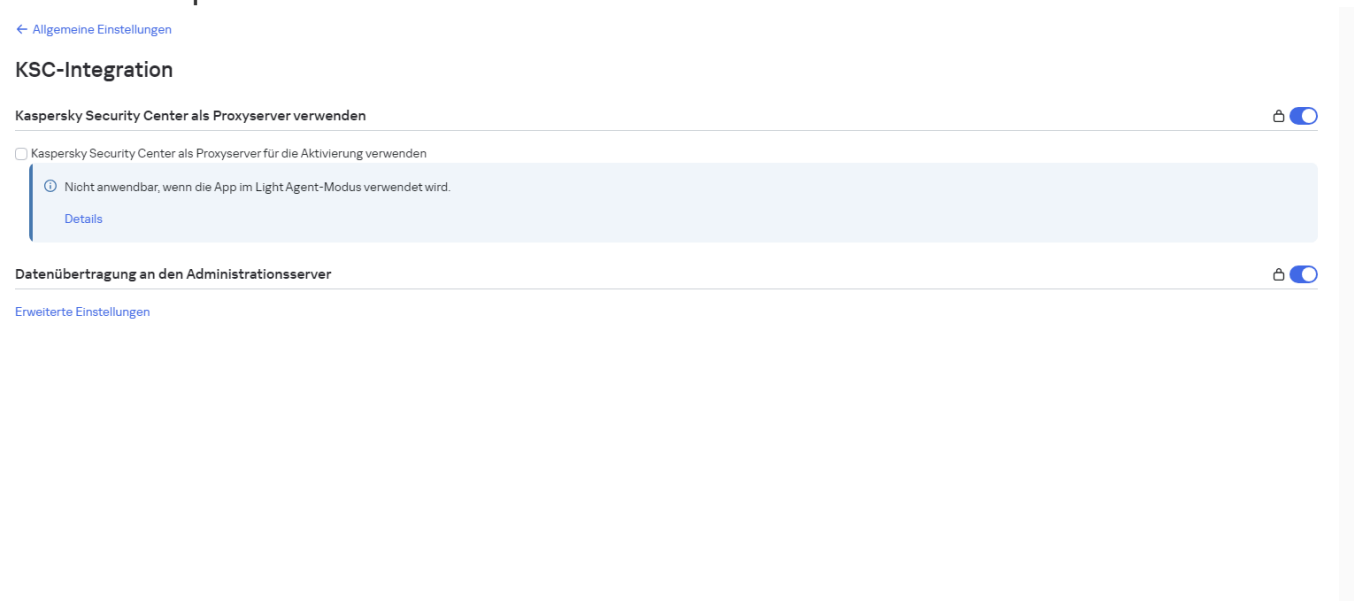
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.

3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.

4. Wechseln Sie zum Abschnitt **Allgemeine Einstellungen** → **KSC-Integration**.

5. Aktivieren Sie das Kontrollkästchen **Kaspersky Security Center als Proxyserver für die Aktivierung verwenden**.

6. Klicken Sie auf **Speichern**.



Integration in Kaspersky Security Center

Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, wird die Verwendung eines Proxyservers für die Verbindung mit Kaspersky Security Network, der SVM und dem Integrationsserver nicht unterstützt. Außerdem wird die Verwendung des Administrationsservers als Proxyserver für den Zugriff auf die Aktivierungsserver von Kaspersky im Light Agent-Modus nicht unterstützt.

So verwalten Sie Proxyserver-Einstellungen in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Allgemeine Einstellungen** → **Netzwerkeinstellungen**.

5. Stellen Sie den Umschalter auf **Proxyserver-Verwendung AKTIVIERT**.

6. Füllen Sie im angezeigten Fenster die Felder aus:

   - **Proxyserver-Adresse**.
   - **Proxyserver-Port**.

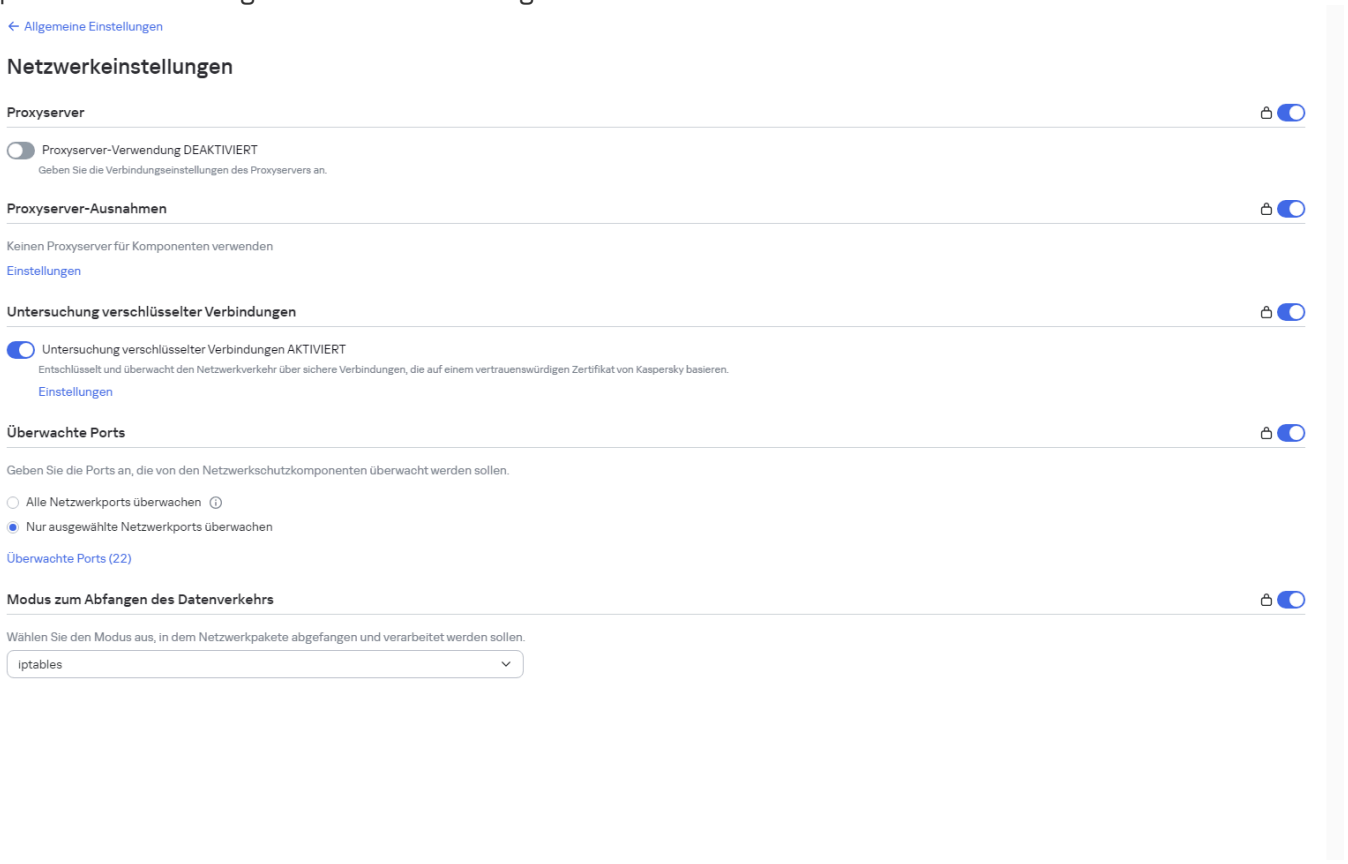
7. Aktivieren Sie bei Bedarf die Proxyserver-Authentifizierung:

   a. Aktivieren Sie das Kontrollkästchen **Proxyserver-Authentifizierung verwenden**.

   b. Füllen Sie die Felder aus:

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

8. Speichern Sie die vorgenommenen Änderungen.



Netzwerkeinstellungen

So verwalten Sie Proxyserver-Einstellungen über die Befehlszeile

1. Führen Sie den folgenden Befehl aus, um die Verwendung eines Proxyservers zu aktivieren:

```
kesl-control --set-net-settings UseProxy=Yes ProxyServer=<proxy server address>
```

2. Führen Sie den folgenden Befehl aus, um die aktuellen Werte der Netzwerkeinstellungen zu überprüfen:

```
kesl-control --get-net-settings
```

Symbole

Befehlsoptionen

Parameter	Description
`ProxyServer`	Adresse des Proxy-Servers, der für die Internetverbindung verwendet wird Adresse des Proxyservers in einem der folgenden Formate: • `[<connection protocol>://]<address of the proxy server>:<port>`, wenn für die Verbindung mit dem Proxyserver keine Authentifizierung erforderlich ist; • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`, wenn für die Verbindung mit dem Proxyserver eine Authentifizierung erforderlich ist. Geben Sie eine IPv6-Adresse in eckigen Klammern ein. Das Herstellen einer Verbindung mit dem Proxyserver über das HTTPS-Protokoll wird nicht unterstützt. 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 verwendet eine unsichere Verbindung und das Benutzerkonto ist möglicherweise kompromittiert.

Proxyserver-Ausnahmen

Wenn Sie für Verbindungen zu bestimmten Adressen keinen Proxyserver verwenden müssen, können Sie diese Adressen zu den Ausnahmen hinzufügen.

Sie können die Verwendung eines Proxyservers auch für die Komponenten EDR Expert (on-premise), NDR (KATA) und Sandbox deaktivieren, welche die Integration mit Detection and Response-Lösungen gewährleisten. Bei der Verbindung mit den Integrationsservern dieser Komponenten wird der Proxyserver nicht verwendet.

So konfigurieren Sie Proxyserver-Ausnahmen in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Netzwerkeinstellungen**.
5. Klicken Sie im Block **Proxyserver-Ausnahmen** auf den Link **Einstellungen**.
   Das Fenster für Proxyserver-Ausnahmen wird geöffnet
6. Aktivieren Sie die Kontrollkästchen für die Komponenten, für die Sie keinen Proxyserver verwenden möchten:
   - **Endpoint Detection and Response Expert (On-Premises)**
   - **KATA Sandbox**.
   - **Network Detection and Response (KATA)**.
7. Fügen Sie IP-Adressen hinzu, für die Sie keinen Proxyserver verwenden möchten. Beispiel: `1.2.3.4/24`, `1234::cdef/96`.
8. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie Proxyserver-Ausnahmen über die Befehlszeile

1. Führen Sie den folgenden Befehl aus, um Adressen hinzuzufügen, für die kein Proxyserver verwendet werden soll:

   ```
   kesl-control --set-net-settings ProxyBypass=<address:port>
   ```

2. Führen Sie den folgenden Befehl aus, um den Proxyserver für Integrationen mit Kaspersky Detection and Response-Lösungen zu umgehen:

   ```
   kesl-control --set-net-settings [ProxyBypassEdr=<Yes|No>] [ProxyBypassNdr=<Yes|No>] [ProxyBypassSandbox=
   <Yes|No>]
   ```

3. Führen Sie den folgenden Befehl aus, um die aktuellen Werte der Netzwerkeinstellungen zu überprüfen:

   ```
   kesl-control --get-net-settings
   ```

Symbole

Befehlsoptionen

Parameter	Description
`ProxyBypass`	Liste mit Adressen, für deren Verbindung kein Proxyserver verwendet wird. Die Adresse wird im Format `<address>[:<port>]` angegeben. Um Adressen anzugeben, können Sie Masken (Symbol `*`) und Kommentare nach dem Symbol `\` verwenden.
`ProxyBypassEdr`	Ob beim Herstellen einer Verbindung mit Integrationsservern für Kaspersky Endpoint Detection and Response Expert (on-premise) ein Proxyserver verwendet wird. Der Proxyserver wird standardmäßig nicht verwendet (`No`).
`ProxyBypassNdr`	Verwendung des Proxyservers bei einer Verbindung mit Servern, welche die Integration mit Kaspersky Network Detection and Response (KATA) gewährleisten. Der Proxyserver wird standardmäßig nicht verwendet (`No`).
`ProxyBypassSandbox`	Verwendung des Proxyservers bei einer Verbindung mit Servern, welche die Integration mit Sandbox gewährleisten. Der Proxyserver wird standardmäßig nicht verwendet (`No`).

So fängt das Programm den Datenverkehr ab

Ein Programm kann in einem von zwei Modi zum Abfangen des Netzwerkverkehrs arbeiten: eBPF oder iptables. Standardmäßig ist der iptables-Modus ausgewählt.

> Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.

Über das Abfangen von Netzwerkverkehr mit eBPF

Im eBPF-Modus erstellt das Programm einen eigenen separaten Netzwerk-Namespace (network linux namespace), in den es Netzwerkpakete mithilfe von eBPF-Programmen umleitet, die mit `tc`-Warteschlangen (linux traffic control) lokaler Netzwerkschnittstellen verknüpft sind. Der umgeleitete Netzwerkverkehr wird anschließend anhand der aktiver Netzwerkaufgaben analysiert und dann an die ursprüngliche Netzwerkschnittstelle zurückgesendet.

Um Daten zwischen Netzwerk-Namensräumen auszutauschen, werden Paare virtueller Netzwerkschnittstellen `veth` werden verwendet (jedes Ende des Paares befindet sich in seinem eigenen Netzwerk-Namensraum):

- Das `kesl_in – kesl_worm_in`-Paar überträgt den Netzwerkverkehr eingehender Verbindungen.
- Das `kesl_out – kesl_worm_out`-Paar überträgt den Netzwerkverkehr ausgehender Verbindungen.

Über diese Schnittstellenpaare wird der Netzwerkverkehr vom Standard-Namensraum in den von der Anwendung zur Überprüfung erstellten Namensraum übertragen und nach der Analyse über diese zurückgesendet.

Der Netzwerkverkehr erreicht diese Schnittstellen von anderen Netzwerkschnittstellen im System nur dann, wenn die Anwendung ausgeführt wird und die Netzwerküberwachung aktiviert ist. Sie können nicht zur Datenübertragung zwischen entfernten Geräten über das Netzwerk verwendet werden.

Über das Abfangen von Netzwerkverkehr mit iptables

Im iptables-Modus erfolgt das Abfangen mithilfe des Kernel-Mechanismus tproxy.

In der PREROUTING-Kette der mangle-Tabelle werden entsprechende Regeln erstellt, die den Datenverkehr an einen speziellen Port weiterleiten, der vom Programm geöffnet wird. Das Programm fügt außerdem zusätzliche Regeln zu verschiedenen Tabellen der Firewall des Betriebssystems hinzu, um Pakete an tproxy weiterzuleiten. Der Netzwerk-Interceptor des Programms befindet sich zwischen dem Client und dem Server, stellt zu beiden jeweils eine separate Verbindung her und untersucht und überträgt den Datenverkehr zwischen ihnen.

Abgefangene eingehende und ausgehende Verbindungen werden mit separaten Markierungen versehen, die Sie in der Konfigurationsdatei kesl.ini ändern können.

Für ausgehende Verbindungen werden zusätzliche Routing-Regeln eingeführt, die ausgehenden Datenverkehr für abgefangene Ports an die Loopback-Schnittstelle in tproxy umleiten.

Auswählen des Modus zum Abfangen des Datenverkehrs

So wählen Sie in der Web Console einen Modus zum Abfangen des Netzwerkverkehrs aus

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Netzwerkeinstellungen**.

5. Wählen Sie unter **Modus zum Abfangen des Datenverkehrs** einen Modus zum Abfangen des Datenverkehrs für das Programm aus:

   - **iptables**. Standardmäßig ausgewählt. Das Programm verwendet das Tool iptables, um den Datenverkehr abzufangen.

   - **eBPF**. Das Programm verwendet die eBPF-Technologie, um den Datenverkehr abzufangen.

6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So wählen Sie in der Befehlszeile einen Modus zum Abfangen des Netzwerkverkehrs aus

1. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control --set-net-settings NetInterceptorMode=<UseEBPF|UseIPTables>
   ```

2. Führen Sie den folgenden Befehl aus, um die aktuellen Werte der Netzwerkeinstellungen zu überprüfen:

   ```
   kesl-control --get-net-setting
   ```

Besonderheiten und Einschränkungen

- Um den Modus zum Abfangen des Datenverkehrs zu ändern, muss die Anwendung neu gestartet werden. Während des Neustarts werden bestehende Netzwerkverbindungen unterbrochen.

- Wenn das Programm den eBPF-Modus nicht zum Abfangen des Netzwerkverkehrs verwenden kann, wird stattdessen der iptables-Modus verwendet.

So konfigurieren Sie die Richtlinie zur Zertifikatsvalidierung

Die Einstellungen zur Untersuchung des Netzwerkverkehrs werden zur Ausführung der Komponenten Schutz vor Web-Bedrohungen, Schutz vor Netzwerkbedrohungen, Schutz vor E-Mail-Bedrohungen und Web-Kontrolle verwendet.

Standardmäßig entschlüsselt und untersucht Schutz vor Web-Bedrohungen den Netzwerkverkehr, der über verschlüsselte Verbindungen übertragen wird. Dazu validiert das Programm die gesamte Zertifikatskette.

Die Richtlinie für die Zertifikatsvalidierung umfasst die folgenden Einstellungen:

- Validierungsmethode (lokal oder über das Internet)

- Zugriff auf Websites mit einem nicht vertrauenswürdigen Zertifikat

- Zugriff auf Websites mit einem Fehler bei der Zertifikatsvalidierung

Wenn das Gerät nicht über eine direkte Internetverbindung verfügt, können Sie die lokale Methode zur Zertifikatsvalidierung auswählen.

Standardmäßig erlaubt das Programm das Herstellen einer Netzwerkverbindung zu einer Domäne mit einem nicht vertrauenswürdigen Zertifikat. Das Programm zeigt eine HTML-Seite mit einer Warnung an und nennt den Grund, aus dem der Besuch der entsprechenden Domäne nicht empfohlen wird (siehe folgende Abbildung). Die HTML-Seite mit der Warnmeldung enthält einen Link, mit dessen Hilfe der Benutzer auf die angeforderte Webressource zugreifen kann.

Wenn eine Drittanbieter-Anwendung oder ein Drittanbieter-Dienst eine Verbindung mit einer Domäne mit einem nicht vertrauenswürdigen Zertifikat herstellt, erstellt das Programm ein eigenes Zertifikat, um den Datenverkehr zu untersuchen. Das neue Zertifikat hat den Status *Nicht vertrauenswürdig*. Dies ist notwendig, um die Drittanbieter-Anwendung vor der nicht vertrauenswürdigen Verbindung zu warnen, da die HTML-Seite in diesem Fall nicht angezeigt und die Verbindung im Hintergrundmodus hergestellt werden kann.

Die Zertifikatsvalidierung kann mit einem Fehler enden. Beispielsweise beim Arbeiten mit Cloud-Speichern oder bei der Validierung selbstsignierter Zertifikate. Standardmäßig fügt das Programm die Domänennamen solcher Websites zu den Ausnahmen hinzu und kontrolliert den verschlüsselten Netzwerkverkehr beim Besuch dieser Domäne nicht. Das Programm generiert außerdem ein Ereignis für den Fehler bei der Untersuchung der verschlüsselten Verbindung.

Die Anzeige einer Liste der Domänen mit Untersuchungsfehlern bei geschützten Verbindungen ist nur auf der lokalen Programmoberfläche möglich.

So konfigurieren Sie die Richtlinie für die Zertifikatsvalidierung in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Netzwerkeinstellungen**.
5. Stellen Sie unter **Untersuchung verschlüsselter Verbindungen** sicher, dass sich der Schalter in der Position **Untersuchung verschlüsselter Verbindungen AKTIVIERT** befindet.

   Wenn der Schalter deaktiviert ist, kann Kaspersky Endpoint Security nicht auf Inhalte von Websites zugreifen, deren Adressen mit `https://` beginnen.
6. Folgen Sie dem Link **Einstellungen** und konfigurieren Sie die Richtlinie für die Zertifikatsvalidierung:

   - **Besuch einer Domäne mit nicht vertrauenswürdigem Zertifikat**. Aktion beim Fund eines nicht vertrauenswürdigen Zertifikats

     - **Verbindung erlauben**. Das Programm erlaubt Verbindungen zu einer Domäne mit einem nicht vertrauenswürdigen Zertifikat. Das Programm zeigt eine HTML-Seite mit einer Warnung an und nennt den Grund, aus dem der Besuch der entsprechenden Domäne nicht empfohlen wird (siehe folgende Abbildung). Die HTML-Seite mit der Warnmeldung enthält einen Link, mit dessen Hilfe der Benutzer auf die angeforderte Webressource zugreifen kann.

     - **Verbindung blockieren**. Beim Besuch einer Domäne mit einem nicht vertrauenswürdigen Zertifikat blockiert Kaspersky Endpoint Security die Netzwerkverbindung und zeigt eine HTML-Seite an, auf der der Grund angezeigt wird, warum diese Domäne blockiert wurde.

- **Beim Besuch einer Domäne mit Untersuchungsfehler wegen verschlüsselten Verbindungen**. Aktion bei einem Fehler der Untersuchung einer verschlüsselten Verbindung:

  - **Erlauben und Domäne zu Ausnahmen hinzufügen**. Wenn bei der Untersuchung einer verschlüsselten Verbindung ein Fehler auftritt, fügt das Programm die Domäne, die den Fehler verursacht hat, zur Liste der Ausnahmen hinzu und überwacht den verschlüsselten Netzwerkverkehr beim Besuch dieser Domäne nicht.

  - **Verbindung blockieren**. Wenn bei der Untersuchung einer verschlüsselten Verbindung ein Fehler auftritt, blockiert Kaspersky Endpoint Security die Netzwerkverbindung.

- **Richtlinie zur Überprüfung von Zertifikaten**. So validiert das Programm Zertifikate:

  - **Vollständige Überprüfung**. Das Programm verwendet das Internet, um die fehlenden Ketten zu prüfen und herunterzuladen, die zur Validierung eines Zertifikats erforderlich sind.

  - **Lokale Überprüfung**. Das Programm validiert das Zertifikat lokal auf dem Computer.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie die Richtlinie für die Zertifikatsvalidierung über die Befehlszeile

1. Um die Untersuchung verschlüsselter Verbindungen zu aktivieren, führen Sie den folgenden Befehl aus:

   ```
   kesl-control --set-net-settings EncryptedConnectionsScan=Yes
   ```

2. Führen Sie den folgenden Befehl aus, um eine Methode zur Zertifikatsvalidierung auszuwählen:

   ```
   kesl-control --set-net-settings CertificateVerificationPolicy=<FullCheck|LocalCheck>
   ```

3. Führen Sie den folgenden Befehl aus, um eine Aktion auszuwählen, die beim Fund eines nicht vertrauenswürdigen Zertifikats ausgeführt werden soll:

   ```
   kesl-control --set-net-settings UntrustedCertificateAction=<Allow|Block>
   ```

4. Führen Sie den folgenden Befehl aus, um eine Aktion auszuwählen, die beim Auftreten eines Fehlers während der Untersuchung einer verschlüsselten Verbindung ausgeführt werden soll:

   ```
   kesl-control --set-net-setting EncryptedConnectionsScanErrorAction=<AddToAutoExclusions|Disconnect>
   ```

5. Führen Sie den folgenden Befehl aus, um die aktuellen Werte der Netzwerkeinstellungen zu überprüfen:

   ```
   kesl-control --get-net-setting
   ```

Symbole

Parameter	Description
`EncryptedConnectionsScan`	Modus für die Untersuchung verschlüsselter Verbindungen: `Yes` (Standardeinstellung). Die Untersuchung verschlüsselter Verbindungen ist aktiviert. `No`. Die Untersuchung verschlüsselter Verbindungen ist deaktiviert.
`CertificateVerificationPolicy`	Richtlinie zur Zertifikatsvalidierung: `FullCheck` (Standardeinstellung). Das Programm verwendet das Internet, um die fehlenden Ketten zu prüfen und herunterzuladen, die zur Validierung eines Zertifikats erforderlich sind. `LocalCheck`. Das Programm validiert das Zertifikat lokal auf dem Computer.
`UntrustedCertificateAction`	Aktion beim Fund eines nicht vertrauenswürdigen Zertifikats `Allow` (Standardeinstellung). Das Programm erlaubt Verbindungen zu einer Domäne mit einem nicht vertrauenswürdigen Zertifikat. Das Programm zeigt eine HTML-Seite mit einer Warnung an und nennt den Grund, aus dem der Besuch der entsprechenden Domäne nicht empfohlen wird (siehe folgende Abbildung). Die HTML-Seite mit der Warnmeldung enthält einen Link, mit dessen Hilfe der Benutzer auf die angeforderte Webressource zugreifen kann. `Block`. Wenn ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat erfolgt, blockiert Kaspersky Endpoint Security den Aufbau einer Netzwerkverbindung. Wenn ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat in einem Browser erfolgt, so zeigt Kaspersky Endpoint Security eine HTML-Seite an. Diese Seite informiert über den Grund, aus dem der Wechsel zu dieser Domäne blockiert wurde.
`EncryptedConnectionsScanErrorAction`	Aktion bei einem Fehler der Untersuchung einer verschlüsselten Verbindung: `AddToAutoExclusions` (Standardeinstellung). Wenn bei der Untersuchung einer verschlüsselten Verbindung ein Fehler auftritt, fügt das Programm die Domäne, die den Fehler verursacht hat, zur Liste der Ausnahmen hinzu und überwacht den verschlüsselten Netzwerkverkehr beim Besuch dieser Domäne nicht. `Disconnect`. Wenn bei der Untersuchung einer verschlüsselten Verbindung ein Fehler auftritt, blockiert Kaspersky Endpoint Security die Netzwerkverbindung.

So konfigurieren Sie überwachte Ports

Während Kaspersky Endpoint Security ausgeführt wird, überwacht die Komponente Schutz vor Netzwerkbedrohungen Daten, die über bestimmte Netzwerkports übertragen werden. Die Liste der vom Programm überwachten Netzwerkports wird entsprechend den Empfehlungen der Kaspersky-Experten konfiguriert.

Die Komponenten Verhaltensanalyse und Exploit-Prävention überwachen zusätzlich Netzwerkports auf das Vorhandensein von Programmprozessen, die die Sicherheit des Computers gefährden können. Informationen über solche Vorgänge ruf das Programm aus den Antiviren-Datenbanken ab.

Sie können die Ports konfigurieren, die das Programm überwachen soll:

- **Alle Netzwerkports überwachen**. Modus zur Überwachung der Netzwerkports, bei dem das Programm die Datenströme überwacht, die über beliebige offene Netzwerkports des Computers laufen.

  Die Angabe dieses Wertes kann die Auslastung des Betriebssystems erheblich erhöhen.

- **Nur ausgewählte Netzwerkports überwachen**. In diesem Überwachungsmodus für Netzwerkports kontrollieren die Schutzkomponenten die ausgewählten Ports des Computers und die Netzwerkaktivität der ausgewählten Programme.

Wenn Sie Netzwerkverbindungen zu einem NFS-Server abfangen möchten, müssen Sie sicherstellen, dass der NFS-Server mit der Option `insecure` gestartet wird (damit er Verbindungen außerhalb des Portbereichs 1–1024 akzeptiert). Andernfalls lehnt der NFS-Server diese Verbindungen möglicherweise ab.

So konfigurieren Sie überwachte Ports in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Netzwerkeinstellungen**.
5. Wählen Sie unter **Überwachte Ports** den Portüberwachungsmodus des Programms aus:
   - **Alle Netzwerkports überwachen**.
   - **Nur ausgewählte Netzwerkports überwachen** (Standardwert).
6. Wenn Sie die Option **Nur ausgewählte Netzwerkports überwachen** ausgewählt haben, konfigurieren Sie die Liste der zu überwachenden Ports:
   a. Klicken Sie auf den Link **Überwachte Ports**.
   b. Bearbeiten Sie die Liste der überwachten Ports.

   > Damit der Schutz vor E-Mail-Bedrohungen funktioniert, müssen in den Netzwerkeinstellungen die Netzwerkports 25, 110, 143, 465, 587, 993 und 995 überwacht werden. Diese Netzwerkports sind standardmäßig in der Liste der überwachten Ports enthalten. Das Entfernen dieser Ports aus der Liste kann die Funktion der Komponente beeinträchtigen.
7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie überwachte Ports über die Befehlszeile

1. Führen Sie den folgenden Befehl aus, um einen Modus für die Portüberwachung auszuwählen:

   ```
   kesl-control --set-net-settings MonitorNetworkPorts=<All|Selected>
   ```
2. Wenn Sie festgelegt haben, dass nur ausgewählte Ports überwacht werden sollen (`MonitorNetworkPorts=Selected`), geben Sie die Liste der zu überwachenden Ports an:

   ```
   kesl-control --set-net-settings NetworkPorts.item_#.PortName=<port name> NetworkPorts.item_#.Port=<port number>
   ```

   Um einen Port aus der Überwachungsliste zu entfernen, bearbeiten Sie die Liste mithilfe einer Konfigurationsdatei.
3. Führen Sie den folgenden Befehl aus, um die aktuellen Werte der Netzwerkeinstellungen zu überprüfen:

   ```
   kesl-control --get-net-settings
   ```

Symbole

Parameter	Description
`MonitorNetworkPorts`	`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.
`PortName`	Beschreibung des Netzwerkports.
`Port`	Nummern der Netzwerkports, welche die App überwachen soll. Mögliche Werte: `1 – 65535`. Damit der Schutz vor E-Mail-Bedrohungen funktioniert, müssen in den Netzwerkeinstellungen die Netzwerkports 25, 110, 143, 465, 587, 993 und 995 überwacht werden. Diese Netzwerkports sind standardmäßig in der Liste der überwachten Ports enthalten. Das Entfernen dieser Ports aus der Liste kann die Funktion der Komponente beeinträchtigen.

Ausnahmen vom Abfangen des Datenverkehrs durch Tools des Betriebssystems

In den Einstellungen der Anwendung "Kaspersky Endpoint Security" können Sie Ausnahmen beim Abfangen des Datenverkehrs basierend auf der Richtung des Datenverkehrs, der IP-Adresse und des Zielports konfigurieren. Wenn mittels dieser Ausnahmen ein Konflikt der Netzwerkkommunikation zwischen Kaspersky Endpoint Security und Client-Anwendungen nicht behoben werden kann, können Sie die spezielle Berechtigungskette für kesl_bypass-Regeln verwenden.

Die kesl_bypass-Kette ist eine spezielle Regelliste, welche von Kaspersky Endpoint Security in der mangle-Tabelle der Firewall des Betriebssystems (iptables/ip6tables) erstellt wird. Mit den Regeln der kesl_bypass-Kette können Sie Datenverkehr vom Abfangen durch Kaspersky Endpoint Security ausschließen. Da die kesl_bypass-Kette dem Prozess zur Verarbeitung von Netzwerkpaketen als erstes hinzugefügt wird, werden die kesl_bypass-Regeln noch vor allen anderen Regeln von iptables verarbeitet.

Im Gegensatz zu den Ausnahmen, die Sie in den Einstellungen von Kaspersky Endpoint Security konfigurieren, ermöglicht die kesl_bypass-Kette die Konfiguration von Ausnahmen nicht nur anhand der Richtung des Datenverkehrs, der IP-Adresse und des Zielports, sondern auch mithilfe anderer Verbindungsparameter.

Das Ändern von Regeln in der kesl_bypass-Kette erfolgt über das Betriebssystem.

Sie können beispielsweise eine Regel zur Kette kesl_bypass hinzufügen, indem Sie den folgenden Befehl ausführen:

```
iptables -t mangle -I kesl_bypass -m tcp -p tcp --dport http -j ACCEPT
```

Diese Regel verhindert, dass Kaspersky Endpoint Security den ein- und ausgehenden HTTP-Datenverkehr für Port 80 und beliebige IP-Adressen abfängt. Dadurch lassen sich potenzielle Konflikte mit vertrauenswürdigen Webdiensten vermeiden.

Wenn in der Kette eine Regel für eine Datenverkehrsausnahme konfiguriert ist, wirkt diese sich auf die Funktion der Komponenten Schutz vor Web-Bedrohungen, Schutz vor Netzwerkbedrohungen und Web-Kontrolle aus.

Wenn die Anwendung entfernt wird, wird die Regelkette kesl_bypass in iptables und ip6tables nur entfernt, wenn sie leer war.

Überwachung von Dateioperationen

Der Modus zum Abfangen von Dateioperationen wirkt sich auf die Komponenten Schutz vor bedrohlichen Dateien und Gerätekontrolle, die Aktion Ausführungsprävention für Objekte und die Aufgabe Untersuchung von Wechseldatenträgern aus.

Wenn der Blockierungsmodus zum Abfangen von Dateivorgängen aktiviert ist

- Die Anwendung kann den Zugriff auf Dateien blockieren, die während der Untersuchung der Komponente „Schutz vor bedrohlichen Dateien“ geprüft werden. Wenn die Untersuchung in der Datei keine Bedrohungen erkennt, erlaubt die Anwendung den Zugriff auf die Datei. Wenn infizierte Objekte erkannt werden, führt das Programm die Aktionen aus, die in der Einstellung **Aktionen beim Erkennen von Bedrohungen** (`ActionOnThreat`) der Komponente „Schutz vor bedrohlichen Dateien“ festgelegt sind.

- Die Anwendung kann den Zugriff auf Dateien auf einem Gerät blockieren, während Gerätekontrolle bestimmt, ob der Zugriff auf das Gerät gewährt werden kann. Die Anwendung gewährt den Zugriff auf Dateien, wenn aufgrund des Untersuchungsergebnisses der Gerätekontrolle der Zugriff auf das Gerät mit den Dateien erlaubt ist.

- Das Programm kann Dateien auf dem Gerät blockieren, während die Ausführungsprävention für Objekte ermittelt, ob diese Dateien ausgeführt werden dürfen. Das Programm lässt die Ausführung von Dateien zu, wenn die Ausführungsprävention für Objekte als Ergebnis der Untersuchung die Ausführung dieser Dateien erlaubt.

- Das Programm kann während der Untersuchung den Zugriff auf Dateien auf dem Wechseldatenträger blockieren. Wenn die Untersuchung in der Datei keine Bedrohungen erkennt, erlaubt die Anwendung den Zugriff auf die Datei. Wenn infizierte Objekte erkannt werden, führt das Programm die Aktionen aus, die in der Einstellung **Aktionen beim Erkennen von Bedrohungen** (`ActionOnThreat`) der Komponente „Schutz vor bedrohlichen Dateien“ festgelegt sind.

Wenn der Blockierungsmodus zum Abfangen von Dateivorgängen deaktiviert ist

- Die Komponente Schutz vor bedrohlichen Dateien wird unabhängig vom ausgewählten Betriebsmodus im Modus Informieren ausgeführt, erlaubt den Zugriff auf Dateien und führt die Untersuchung asynchron durch.

- Die Komponente Gerätekontrolle wird unabhängig vom ausgewählten Betriebsmodus im Modus Informieren ausgeführt und erlaubt immer den Zugriff auf Geräte.

- Die Aktion Ausführungsprävention für Objekte wird unabhängig vom ausgewählten Betriebsmodus im Modus Informieren ausgeführt und erlaubt immer die Ausführung von Objekten.

- Das Programm erlaubt jederzeit den Zugriff auf Dateien auf dem Wechseldatenträger und führt die Untersuchung asynchron durch.

Diese Art des Abfangens von Dateivorgängen wirkt sich weniger stark auf die Systemleistung aus. Allerdings werden in diesem Fall in Dateien gefundene Bedrohungen weder desinfiziert noch gelöscht. Dies ist beispielsweise möglich, wenn es dem mit der Datei verknüpften Prozess während einer Untersuchung gelingt, die Datei umzubenennen, bevor das Programm über den Status der Datei entscheidet. Sie können die Aufgabe Schadsoftware-Untersuchung ausführen, um solche Bedrohungen später zu verarbeiten.

Standardmäßig ist der Modus zum blockierenden Abfangen von Dateioperationen aktiviert.

So konfigurieren Sie den Modus zum Abfangen von Dateivorgängen in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Erkennungseinstellungen**.
5. Deaktivieren oder aktivieren Sie unter **Modus zum Abfangen von Dateivorgängen** das Kontrollkästchen **Zugriff auf Dateien während der Untersuchung blockieren**. Dieses Kontrollkästchen ist standardmäßig aktiviert.
6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den Modus zum Abfangen von Dateivorgängen über die Befehlszeile

Über die Befehlszeile können Sie den Modus des Interceptors von Dateioperationen mithilfe des Parameters `FileBlockDuringScan` in den allgemeinen Einstellungen der Anwendung konfigurieren.

Um den Modus zum Abfangen von Dateioperationen auszuwählen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings FileBlockDuringScan=<Yes|No>
```

Symbole

Befehlsoptionen

Einstellung	Description
`FileBlockDuringScan`	`Yes` (Standardwert), um den Zugriff auf Dateien zu blockieren, während sie von den Komponenten Schutz vor bedrohlichen Dateien und Gerätekontrolle, der Aktion Ausführungsprävention und der Aufgabe Untersuchung von Wechseldatenträgern untersucht werden. `No` – Zugriff auf Dateien während des Untersuchung nicht blockieren. Der Zugriff auf eine beliebige Datei ist erlaubt, die Überprüfung erfolgt im asynchronen Modus.

Abfangen von Systemereignissen konfigurieren

Sie können in der Web Console, über die Befehlszeile oder in der Verwaltungskonsole einen Mechanismus zum Abfangen von Systemereignissen auswählen.

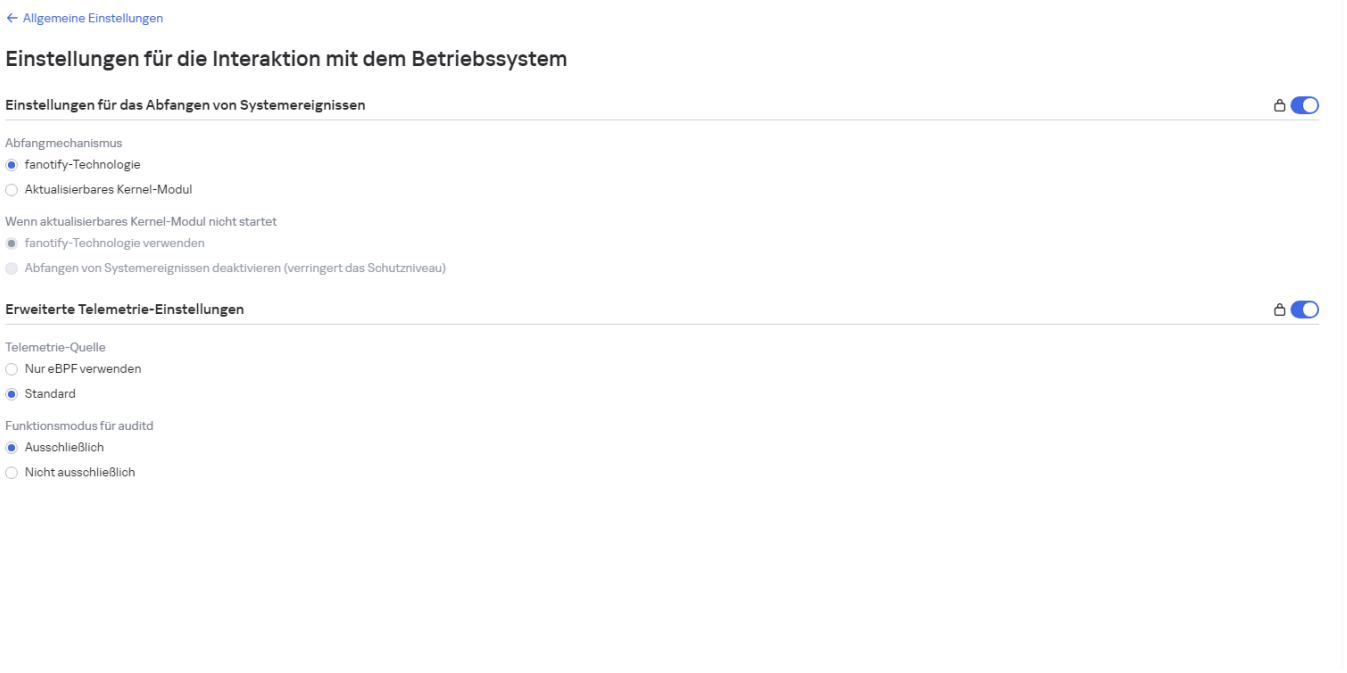
Sie können die Einstellungen für das Abfangen von Systemereignissen nur auf Geräten verwalten, deren Betriebssystem die fanotify-Technologie unterstützt.

Das Konfigurieren des Abfangens von Systemereignissen ist für Geräte mit einer Elbrus-CPU nicht verfügbar.

So konfigurieren Sie den Mechanismus zum Abfangen von Systemereignissen in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Einstellungen für die Interaktion mit dem Betriebssystem**.
5. Wählen Sie unter **Einstellungen für das Abfangen von Systemereignissen** einen Mechanismus zum Abfangen von Systemereignissen aus:
   - **fanotify-Technologie**.
   - **Aktualisierbares Kernel-Modul**. Wenn diese Option ausgewählt ist, wählen Sie die Aktion aus, die das Programm ausführen soll, wenn das aktualisierbare Kernel-Modul nicht gestartet werden kann:
     - **fanotify-Technologie verwenden**.
     - **Abfangen von Systemereignissen deaktivieren (verringert das Schutzniveau)**.



Konfiguration der Kommunikation mit dem Betriebssystem

So konfigurieren Sie den Mechanismus zum Abfangen von Systemereignissen über die Befehlszeile

1. Um einen Mechanismus zum Abfangen von Systemereignissen auszuwählen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings InterceptorMode=<UseFanotify|UseUpdatableKernelModule>
```

2. Um festzulegen, welche Aktion das Programm ausführt, wenn das aktualisierbare Kernel-Modul nicht gestartet werden kann, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings InterceptorFallbackStrategy=<FallbackToFanotify|FallbackToLimitedMode>
```

3. Führen Sie den folgenden Befehl aus, damit das Programm neu gestartet wird, wenn das aktualisierbare Kernel-Modul nicht gestartet werden kann:

```
kesl-control --set-app-settings InterceptorApplyStrategy=<RestartServiceAutomatically|RestartServiceManually>
```

4. Um die aktuellen Anwendungseinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-app-settings [--json]
```

Symbole

Befehlsoptionen

Parameter	Description
`InterceptorMode`	`UseFanotify` (Standardwert) – fanotify-Technologie zum Abfangen von Systemereignissen verwenden. `UseUpdatableKernelModule` – Aktualisierbares Kernel-Modul zum Abfangen von Systemereignissen verwenden.
`InterceptorFallbackStrategy`	`FallbackToFanotify` (Standardwert) – Zur Verwendung der fanotify-Technologie zum Abfangen von Systemereignissen übergehen. `FallbackToLimitedMode` – Systemereignisse nicht abfangen. Wenn das Abfangen von Systemereignissen von der Anwendung nicht verwendet wird, findet keine Dateiuntersuchung in Echtzeit statt. Dies reduziert die Schutzstufe des Geräts.
`InterceptorApplyStrategy`	`RestartServiceAutomatically` (empfohlener Wert) – Anwendung automatisch neu starten, um das aktualisierbare Kernel-Modul zu starten. Wir empfehlen, diese Einstellung zu verwenden. `RestartServiceManually` (Standard) startet das aktualisierbare Kernel-Modul, nachdem das Programm vom Benutzer manuell neu gestartet wurde.

Das Programm kann den Mechanismus zum Abfangen verwenden, der auf dem aktualisierbaren Kernel-Modul basiert, wenn das Betriebssystem die Anforderungen für die Installation des aktualisierbaren Kernel-Moduls erfüllt.

Wenn Sie als Abfangmechanismus das aktualisierbare Kernel-Modul ausgewählt haben, können Sie das Verhalten der Anwendung für den Fall konfigurieren, in dem beim Starten des Kernel-Moduls ein Fehler auftritt und das Modul nicht gestartet wird. In diesem Fall kann die Anwendung auf die fanotify-Technologie wechseln, Systemereignissen abzufangen, oder das Abfangen von Systemereignissen komplett deaktivieren.

Wenn das aktualisierbare Kernel-Modul während der Programminstallation nicht installiert werden konnte, können Sie es später installieren, sobald die Unterstützung für Ihr Betriebssystem verfügbar ist. Um dies zu tun:

1. Aktualisieren Sie die Datenbanken und Module der Anwendung Das aktualisierbare Kernel-Modul wird im Rahmen des Updates installiert.

2. Wählen Sie den Abfangmechanismus auf Basis des aktualisierbaren Kernel-Moduls.

Die Anwendung kann in den folgenden Fällen zur Verwendung des aktualisierbaren Kernel-Moduls übergehen:

- Wenn Sie in den Anwendungseinstellungen den Mechanismus zum Abfangen von Systemereignissen auf das aktualisierbare Kernel-Modul geändert haben.
- Wenn auf einem Gerät, auf dem das aktualisierbare Kernel-Modul nicht gestartet wurde, die im Rahmen von Updates empfangenen Datenbank- und Modul-Updates eine Unterstützung für das aktualisierbare Kernel-Modul bieten.

Informationen zum Status des aktualisierbaren Kernel-Moduls

Informationen zum Status und zur Verfügbarkeit des aktualisierbaren Kernel-Moduls werden in Form von Statusmeldungen angezeigt:

- **Gestartet** bedeutet, dass das Modul installiert ist und ausgeführt wird.
- **Angehalten** bedeutet, dass das Modul installiert ist, aber nicht ausgeführt wird.
- **Nicht verfügbar** bedeutet, dass das Modul auf dem Gerät nicht unterstützt wird.
- **Ausführungsfehler** bedeutet, dass beim Starten des Moduls ein Fehler aufgetreten ist und das Modul nicht ausgeführt wird.

Sie können den Status des aktualisierbaren Kernel-Moduls auf dem Gerät in der Web Console und über die Befehlszeile anzeigen.

So zeigen Sie den Status des aktualisierbaren Kernel-Moduls in der Web Console an

1. Wählen Sie im Hauptfenster der Web Console **Asset-Management** → **Assets (Geräte)** aus.

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Um eine verschachtelte Gruppe auszuwählen, klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Hierarchie anzeigen**.

   In der Liste werden nur die verwalteten Geräte der ausgewählten Administrationsgruppe angezeigt.

3. Klicken Sie auf den Namen eines Geräts.
4. Wechseln Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts zur Registerkarte **Anwendungen**.
5. Klicken Sie in der Liste der auf dem Gerät installierten Anwendungen auf den Namen der Anwendung Kaspersky Endpoint Security.
6. Zeigen Sie den Status der Funktionskomponente **Aktualisierbares Kernel-Modul** an.

So zeigen Sie den Status des aktualisierbaren Kernel-Moduls über die Befehlszeile an

Um den Status des aktualisierbaren Kernel-Moduls anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --app-info [--json]
```

Dabei bedeutet `--json` die Ausgabe von Daten im JSON-Format. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen in die Konsole ausgegeben.

"Abgesicherter" Modus bei Verwendung des aktualisierbaren Kernel-Moduls

Wenn das Programm bei Verwendung des aktualisierbaren Kernel-Moduls instabil ist, wechselt das Programm nach Erreichen der angegebenen maximalen Anzahl abnormaler Beendigungen automatisch in den „abgesicherten“ Modus (`SafeMode=yes` wird in der Konfigurationsdatei kesl.ini festgelegt). Standardmäßig wechselt die Anwendung nach drei Abstürzen in den "abgesicherten" Ausführungsmodus. Die maximale Anzahl abnormaler Beendigungen wird in der Einstellung `PanicThreshold` in der Konfigurationsdatei kesl.ini festgelegt.

Wenn die Anwendung im "abgesicherten" Modus ausgeführt wird, wird das aktualisierbare Kernel-Modul nicht gestartet. Stattdessen verwendet die Anwendung die fanotify-Technologie, um Systemereignisse abzufangen. Das Programm sendet das Tag `UpdatableKernelModule=Error` an Kaspersky Security Center.

Um das aktualisierbare Kernel-Modul nach der Behebung der Probleme mit dem Programm weiterhin zu verwenden, müssen Sie den „abgesicherten“ Modus deaktivieren.

So deaktivieren Sie den abgesicherten Modus des Programms über die Befehlszeile

1. Öffnen Sie die Datei /var/opt/kaspersky/kesl/common/kesl.ini zur Bearbeitung.
2. Legen Sie im Abschnitt `[General]` den Parameterwert `SafeMode=no` fest.
3. Starten Sie Kaspersky Endpoint Security neu:

   ```
   systemctl restart kesl
   ```

Der abgesicherte Modus ist deaktiviert.

Erweiterte Einstellungen für Telemetriedaten konfigurieren

Sie können die folgenden zusätzlichen Parameter für die Erfassung von Telemetriedaten konfigurieren, die an integrierte Detection and Response-Lösungen gesendet werden:

- Quelle der Telemetriedaten. Zur Erfassung von Telemetriedaten können Sie die eBPF-Technologie zusammen mit dem auditd-Dienst oder nur die eBPF-Technologie verwenden.
- Nutzungsmodus des auditd-Dienstes. Kaspersky Endpoint Security kann den auditd-Dienst entweder im exklusiven Modus oder im Multicast-Modus nutzen.

So konfigurieren Sie zusätzliche Einstellungen für Telemetriedaten in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Einstellungen für die Interaktion mit dem Betriebssystem**.

5. Geben Sie unter **Einstellungen für Telemetriedaten** die Quelle an, die Kaspersky Endpoint Security zum Erfassen von Telemetriedaten verwendet:

   - **Nur eBPF verwenden** – Zur Erfassung von Telemetriedaten wird ausschließlich die eBPF-Technologie verwendet.

     Wenn die Option **Nur eBPF verwenden** ausgewählt ist, können Telemetriedaten für Detection and Response-Lösungen Einschränkungen unterliegen.

   - **Standard** bedeutet, dass die eBPF-Technologie und der auditd-Dienst zum Abrufen von Telemetriedaten verwendet werden.

6. Geben Sie außerdem den Modus des auditd-Dienstes an:

   - **Exklusiv** bedeutet, dass Kaspersky Endpoint Security den auditd-Dienst im exklusiven Modus verwendet.
   - **Nicht exklusiv** bedeutet, dass der auditd-Dienst im nicht exklusiven Modus verwendet wird.

     Diese Einstellung wird nur angewendet, wenn **Quelle für Telemetriedaten** auf **Standardmäßig** festgelegt ist.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie zusätzliche Einstellungen für Telemetriedaten über die Befehlszeile

Auf der Befehlszeile können Sie zusätzliche Einstellungen für Telemetriedaten mithilfe der Einstellungen `TelemetrySource` und `UseTelemetryMonopolyMode` der vordefinierten Aufgabe Behavior Detection verwalten.

1. Um die Quelle für Telemetriedaten zu aktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 20 TelemetrySource=<Default|OnlyEBPF>
```

2. Um einen Modus für den auditd-Dienst auszuwählen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 20 UseTelemetryMonopolyMode=<True|False>
```

Symbole

Befehlsoptionen

Parameter	Description
`TelemetrySource`	`Default` (Standardwert) – Zur Erfassung von Telemetriedaten wird die eBPF-Technologie und der auditd-Dienst verwendet. `OnlyEBPF` – Zur Erfassung von Telemetriedaten wird nur die eBPF-Technologie verwendet.
`UseTelemetryMonopolyMode`	`True` (Standardwert) – Die Anwendung "Kaspersky Endpoint Security" verwendet den Dienst "auditd" im exklusiven Modus. `False` bedeutet, dass der Dienst auditd im nicht-exklusiven Modus verwendet wird. Der Parameter `UseTelemetryMonopolyMode` wird nur angewendet, wenn für den Parameter `TelemetrySource` der Wert `Default` angegeben wurde.

Datenverwaltung

Wenn die Anwendung Kaspersky Endpoint Security während der Untersuchung eines geschützten Geräts bösartigen Code in einer Datei erkennt, kann die Anwendung die Datei blockieren, ihr den Status *Infiziert* zuweisen, eine Kopie der Datei 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.

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 Backup-Kopie wiederherzustellen.

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.

Backup-Einstellungen konfigurieren

Sie können die Backup-Einstellungen auf einem Gerät in der Web Console, in der Verwaltungskonsole oder über die Befehlszeile verwalten. Sie können die folgenden Backup-Einstellungen konfigurieren:

- **Speicherzeit von Objekten im Backup.** Standardmäßig werden Objekte 30 Tage lang gespeichert. Nach Ablauf der maximalen Speicherdauer löscht Kaspersky Endpoint Security die ältesten Dateien aus dem Backup.
- **Maximale Backup-Größe.** Standardmäßig ist die folgende maximale Backup-Größe konfiguriert:
  - 0 MB, wenn keine Richtlinie angewendet wird
  - 1024 MB, wenn eine Richtlinie angewendet wird

  Nach Erreichen der maximalen Backup-Größe löscht Kaspersky Endpoint Security automatisch die ältesten Dateien. Dadurch ist gewährleistet, dass die maximale Backup-Größe nicht überschritten wird.
- **Pfad zum Verzeichnis, in dem Backup- und Quarantäne-Objekte gespeichert werden** (kann nur über die Befehlszeile konfiguriert werden). Standardmäßig wird das Verzeichnis /var/opt/kaspersky/kesl/common/objects-backup/ zum Speichern von Backup-Kopien von Dateien und Dateien in Quarantäne verwendet.

So konfigurieren Sie Backup-Einstellungen in der Web Console

So verwalten Sie Backup-Einstellungen in den Richtlinieneigenschaften:

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Allgemeine Einstellungen → Berichte und Speicher**.
5. Konfigurieren Sie im Abschnitt **Backup** die folgenden Einstellungen:

   - **Objekte löschen nach (Tagen)**. Ist das Kontrollkästchen aktiviert, so ist die maximale Speicherdauer für Dateien durch das festgelegte Zeitintervall beschränkt. Dieses Kontrollkästchen ist standardmäßig aktiviert.

     Mögliche Werte: 0 bis 10000.

   - **Maximale Größe des Backup-Speichers (MB)**. Ist das Kontrollkästchen aktiviert, so ist die maximale Backup-Größe durch den festgelegten Wert beschränkt. Dieses Kontrollkästchen ist standardmäßig aktiviert.

     Mögliche Werte: 1 bis 4000.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So verwalten Sie Backup-Einstellungen in den Eigenschaften des verwalteten Geräts:

1. Wählen Sie im Hauptfenster der Web Console **Asset-Management → Assets (Geräte)** aus.

   Die Liste der verwalteten Geräte wird geöffnet.
2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Um eine verschachtelte Gruppe auszuwählen, klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Hierarchie anzeigen**.

   In der Liste werden nur die verwalteten Geräte der ausgewählten Administrationsgruppe angezeigt.
3. Klicken Sie auf den Namen eines Geräts.
4. Wechseln Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts zur Registerkarte **Anwendungen**.
5. Wählen Sie Kaspersky Endpoint Security aus
6. Wechseln Sie zu **Programmeinstellungen → Speichereinstellungen**.

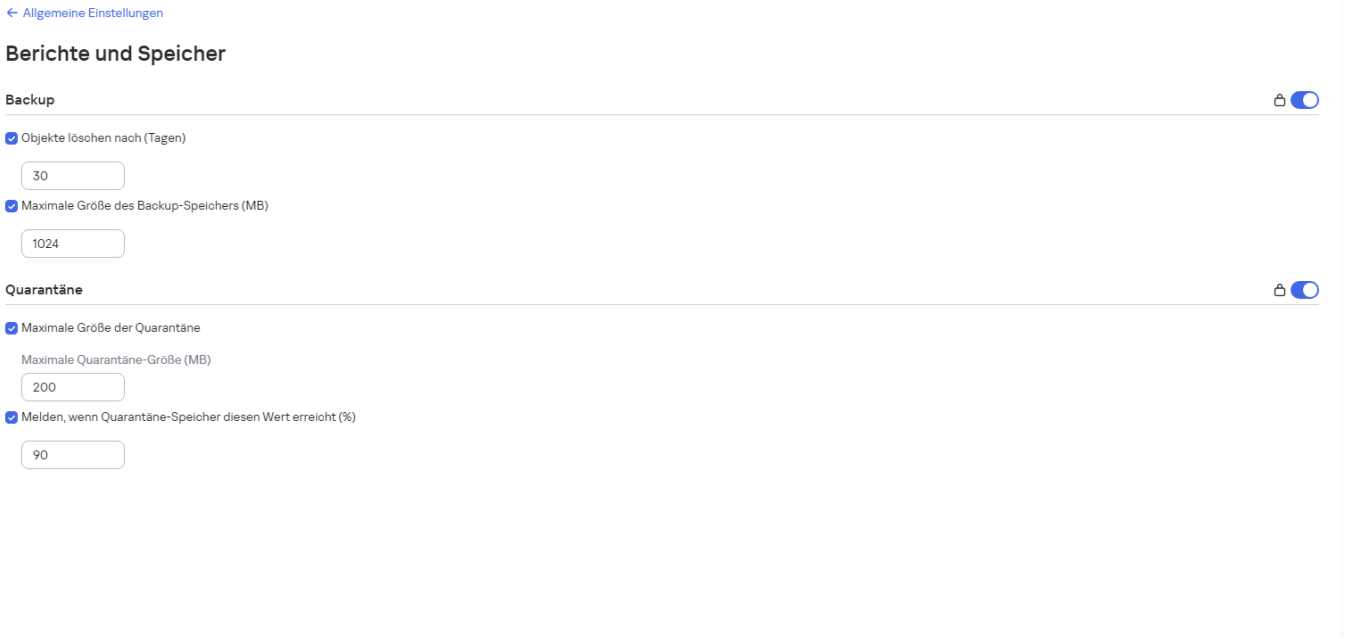
   - **Objekte löschen nach (Tagen)**. Ist das Kontrollkästchen aktiviert, so ist die maximale Speicherdauer für Dateien durch das festgelegte Zeitintervall beschränkt. Dieses Kontrollkästchen ist standardmäßig aktiviert.

     Mögliche Werte: 1 bis 10000.

   - **Maximale Größe des Backup-Speichers (MB)**. Ist das Kontrollkästchen aktiviert, so ist die maximale Backup-Größe durch den festgelegten Wert beschränkt. Dieses Kontrollkästchen ist standardmäßig aktiviert.

     Mögliche Werte: 1 bis 4000.

7. Speichern Sie die vorgenommenen Änderungen.



Berichte und Speicher

So konfigurieren Sie das Backup über die Befehlszeile

Über die Befehlszeile können Sie die Backup-Einstellungen mithilfe der Optionen `BackupDaysToLive`, `BackupSizeLimit` und `QuarantineBackupFolder` in den allgemeinen Anwendungseinstellungen konfigurieren.

1. Führen Sie den folgenden Befehl aus, um den Aufbewahrungszeitraum für Objekte im Backup anzupassen:

```
kesl-control --set-app-settings BackupDaysToLive=<days>
```

2. Führen Sie den folgenden Befehl aus, um die maximale Größe des Backups anzupassen:

```
kesl-control --set-app-settings BackupSizeLimit=<Backup size>
```

3. Führen Sie den folgenden Befehl aus, um das Verzeichnis anzupassen, in dem die Backup- und Quarantäne-Objekte gespeichert werden:

```
kesl-control --set-app-settings QuarantineBackupFolder=<path to folder>
```

4. Um die aktuellen Anwendungseinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-app-settings
```

Befehlsoptionen

Parameter	Description
`BackupDaysToLive`	Speicherzeit von Objekten im Backup (in Tagen) Nach Ablauf des angegebenen Zeitraums löscht die Anwendung die ältesten Backup-Dateien. Um die Begrenzung der Speicherzeit von Objekten im Backup aufzuheben, geben Sie den Wert 0 an.
`BackupSizeLimit`	Maximale Backup-Größe (in Megabyte) Wenn die maximale Größe des Backups erreicht ist, löscht die Anwendung die ältesten Backup-Dateien. Um die Begrenzung der Backup-Größe aufzuheben, geben Sie den Wert 0 an.

Parameter	Description
`QuarantineBackupFolder`	Pfad zum Verzeichnis, in dem die Objekte des Backups und der Quarantäne gespeichert werden. Sie können ein Verzeichnis angeben, das sich vom Standardverzeichnis unterscheidet. Die zum Speichern der Objekte des Backups und der Quarantäne verwendeten Verzeichnisse können sich auf beliebigen Geräten befinden. Es wird nicht empfohlen, Verzeichnisse zu wählen, die sich auf Remote-Geräten befindet und etwa über Samba- oder NFS-Protokolle gemountet sind. Wenn das angegebene Verzeichnis nicht existiert oder nicht verfügbar ist, verwendet die Anwendung das Standardverzeichnis. Der Standardwert ist `/var/opt/kaspersky/kesl/common/objects-backup/` Für den Zugriff auf das Standardverzeichnis sind Root-Rechte erforderlich.

Objekte im Backup anzeigen

Eine allgemeine Liste der Dateien, die von Kaspersky-Anwendungen auf Client-Geräten im Backup abgelegt werden, wird in Kaspersky Security Center erstellt und ist in der Web Console und in der Verwaltungskonsole (**Erweitert** → **Speicher** → **Backup**) verfügbar.

Kaspersky Security Center kopiert keine Dateien vom Backup auf den Administrationsserver; alle Dateien werden im Backup auf geschützten Geräten abgelegt.

So zeigen Sie in der Web Console Informationen über Objekte im Backup an

1. Wählen Sie im Hauptfenster der Web Console **Datenverwaltungen** → **Datei-Backups** aus.

   Dadurch wird eine Liste der Dateien geöffnet, die von Kaspersky-Programmen auf Client-Geräten im Backup abgelegt wurden. Kaspersky Security Center kopiert keine Dateien vom Backup auf den Administrationsserver; alle Dateien werden im Backup auf geschützten Geräten abgelegt.

2. Zeigen Sie die Eigenschaften von Dateien im Backup-Speicher auf geschützten Geräten an:

   - **Dateiname**
   - **Status**:
     - *Warnung*
     - *Wahrscheinlich infiziert*
     - *Vom Benutzer hinzugefügt*
     - *Fehlalarm*
     - *Desinfiziert*
     - *Nicht infiziert*
     - *Kennwortgeschützt*
     - *Gelöscht*
     - *Muss an Kaspersky gesendet werden*

- **Gerätename**
- **Ausgeführte Aktion**:
  - *Löschen*
  - *Desinfektion*
  - *Untersuchung*
  - *Wiederherstellung*
- **Objekt**
- **Im Speicher abgelegt**
- **Eintrag hinzugefügt von**
- **Größe (Byte)**
- **Ordner wiederhergestellt**
- **Benutzer**
- **Description**
- **Name des virtuellen Administrationsservers**

So zeigen Sie Informationen zu Objekten im Backup über die Befehlszeile an

Um Informationen zu Backup-Objekten anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control -B --query ["<filter conditions>"] [-n <objects number>] [--json]
```

Wobei gilt:

- `<filter conditions>` gibt einen oder mehrere logische Ausdrücke im Format `<field> <comparison operator> '<value>'` an, die mit dem logischen Operator `and` kombiniert werden, um die Ergebnisse der Abfrage einzuschränken. Wenn Sie keine Filterbedingungen angeben, zeigt die App Informationen zu allen Backup-Objekten an.
- `<objects number>` gibt an, wie viele der neuesten Objekte im Speicher angezeigt werden sollen. Wenn Sie den Schlüssel `-n` nicht angeben, zeigt die Anwendung Informationen über die letzten 30 Objekte an. Wenn Sie Informationen über alle Objekte ausgeben möchten, geben Sie den Wert `0` an.
- `--json` – Gibt Daten im JSON-Format aus.

In der Zeile `ObjectId` wird die numerische ID angezeigt, welche die Anwendung 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.

So zeigen Sie Informationen zu Objekten im Backup in der grafischen Benutzeroberfläche an

1. Öffnen Sie das Hauptfenster der grafischen Benutzeroberfläche des Programms.
2. Klicken Sie im unteren Bereich des Hauptfensters der Anwendung auf die Schaltfläche **Backup**.

   Das Fenster **Backup** wird geöffnet.

Im Fenster werden folgende Informationen zu den Objekten im Backup angezeigt:

- Name des Objekts
- Den vollständigen Pfad zu einem 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)
- Die Objektgröße.

Objekte aus dem Backup wiederherstellen

Die in das Backup verschobenen Dateien werden gemäß den angegebenen Parametern an ihren ursprünglichen Speicherorten wiederhergestellt. Das Mandanten-Tag (nur auf Geräten mit dem Betriebssystem Astra Linux) und die Attribute der ursprünglichen Datei (mit Ausnahme der Attribute "immutable" und "append-only") werden bei der Wiederherstellung beibehalten.

Auf Geräten mit dem Betriebssystem Astra Linux schlägt die Wiederherstellung einer Datei aus einem Backup fehl, wenn:

- Das Mandanten-Tag der Datei höher ist als das Mandanten-Tag des Verzeichnisses, in dem die Datei wiederhergestellt wird.
- Das Mandanten-Tag der Datei niedriger ist als das Mandanten-Tag des Verzeichnisses, in dem die Datei wiederhergestellt wird, und für das Verzeichnis das Flag "ccnr" nicht angegeben ist.
- Auf Geräten mit dem Betriebssystem Astra Linux kann im Modus für geschlossene Softwareumgebungen eine Datei nur unter dem Benutzerkonto wiederhergestellt werden, unter dem sie ins Backup verschoben wurde. Beim Wiederherstellen einer Datei erstellt die Anwendung ein Verzeichnis mit MAC-Label 3 (cnnr-Flag).

Um Aktionen mit Dateien im Backup-Speicher in Kaspersky Security Center durchzuführen, müssen Sie die Übertragung von Daten über Backup-Dateien an den Administrationsserver aktivieren.

Die Wiederherstellung infizierter Objekte kann zu einer Infektion des Geräts führen.

So stellen Sie in der Web Console Objekte aus dem Backup wieder her

1. Wählen Sie im Hauptfenster der Web Console **Datenverwaltungen** → **Datei-Backups** aus.

   Dadurch wird eine Liste der Dateien geöffnet, die von Kaspersky-Programmen auf Client-Geräten im Backup abgelegt wurden. Kaspersky Security Center kopiert keine Dateien vom Backup auf den Administrationsserver; alle Dateien werden im Backup auf geschützten Geräten abgelegt.

2. Aktivieren Sie die Kontrollkästchen neben den Dateien, die Sie wiederherstellen möchten.

3. Klicken Sie auf **Wiederherstellen**.

   Backup-Objekte auf Client-Geräten werden wiederhergestellt.

So stellen Sie Objekte aus dem Backup über die Befehlszeile wieder her

So stellen Sie ein Objekt unter dem ursprünglichen Namen am ursprünglichen Speicherort wieder her:

```
kesl-control -B --restore <object id>
```

Dabei ist `<object id>` die numerische ID, die das Programm dem Objekt beim Ablegen im Backup zugewiesen hat.

Um das Objekt unter einem neuen Namen in einem angegebenen Verzeichnis wiederherzustellen, führen Sie den folgenden Befehl aus:

```
kesl-control -B --restore <object id> --file <path to file>
```

Dabei ist `--file <path to file>` der neue Name der Datei 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.

Auf Geräten mit dem Betriebssystem Astra Linux kann im Modus für geschlossene Softwareumgebungen eine Datei nur unter dem Benutzerkonto wiederhergestellt werden, unter dem sie ins Backup verschoben wurde.

So stellen Sie Objekte aus dem Backup in der grafischen Benutzeroberfläche wieder her

So stellen Sie Objekte aus dem Backup in ihren ursprünglichen Verzeichnissen wieder her:

1. Öffnen Sie das Hauptfenster der grafischen Benutzeroberfläche des Programms.

2. Klicken Sie im unteren Bereich des Hauptfensters der Anwendung auf die Schaltfläche **Backup**.

   Das Fenster **Backup** wird geöffnet.

3. Wählen Sie die Objekte aus, die Sie wiederherstellen möchten.

4. Klicken Sie auf **Wiederherstellen**.

Die Objekte aus dem Backup werden wiederhergestellt und stehen im ursprünglichen Verzeichnis zur Verfügung.

Informationen über die Wiederherstellung und Löschung von Objekten im Ereignisprotokoll aufzeichnen.

Objekte aus dem Backup löschen

Nach Ablauf des angegebenen Zeitraums oder bei Erreichen der maximalen Backup-Größe löscht die App automatisch die ältesten Backup-Dateien mit beliebigem Status aus dem Backup.

Sie können eine Backup-Kopie sowohl einer wiederhergestellten als auch einer nicht wiederhergestellten Datei auch selbst löschen.

So löschen Sie Objekte aus dem Backup in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Datenverwaltungen** → **Datei-Backups** aus.

   Dadurch wird eine Liste der Dateien geöffnet, die von Kaspersky-Programmen auf Client-Geräten im Backup abgelegt wurden. Kaspersky Security Center kopiert keine Dateien vom Backup auf den Administrationsserver; alle Dateien werden im Backup auf geschützten Geräten abgelegt.

2. Aktivieren Sie die Kontrollkästchen neben den Dateien, die Sie löschen möchten.

3. Klicken Sie auf **Löschen**.

Backup-Objekte auf Client-Geräten werden gelöscht.

So löschen Sie Objekte aus dem Backup über die Befehlszeile

Um ausgewählte Objekte aus dem Backup zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control -B --mass-remove --query "<filter conditions>"
```

wobei `<filter conditions>` einen oder mehrere logische Ausdrücke im Format `<field> <comparison operator> '<value>'` angibt, die mit dem logischen Operator `and` kombiniert werden, um die Ergebnisse der Abfrage einzuschränken.

Beispiele:

```
Objekt mit ID=15 löschen
```

```
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

```
Objekte löschen, 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
```

So löschen Sie Objekte aus dem Backup in der grafischen Benutzeroberfläche

1. Öffnen Sie das Hauptfenster der grafischen Benutzeroberfläche des Programms.

2. Klicken Sie im unteren Bereich des Hauptfensters der Anwendung auf die Schaltfläche **Backup**.

   Das Fenster **Backup** wird geöffnet.

3. Wählen Sie die Objekte aus, die Sie löschen möchten.

4. Klicken Sie auf **Löschen**.

Backup-Objekte werden gelöscht. Entfernte Objekte können später nicht wiederhergestellt werden.

Informationen über die Wiederherstellung und Löschung von Objekten im Ereignisprotokoll aufzeichnen.

Schutz vor komplexen Bedrohungen und gezielten Angriffen

Kaspersky Detection and Response-Lösungen sind Sicherheitssysteme zur Erkennung komplexer Bedrohungen und Angriffsindikatoren auf verschiedenen Ebenen einer Unternehmensinfrastruktur. Detection and Response-Lösungen liefern Informationen über erkannte Bedrohungen und ermöglichen Ihnen, Ihre Reaktion auf Erkennungen zu verwalten.

Kaspersky Endpoint Security kann mit den folgenden Lösungen Detection and Response von Kaspersky interagieren:

- Kaspersky Endpoint Detection and Response Expert (on-premise) auf der Open Single Management Platform (OSMP). Die Integration erfolgt durch die Programmkomponente Endpoint Detection and Response Expert (on-premise) von Kaspersky Endpoint Security (im Folgenden auch *EDR Expert (on-premise)* genannt).

- Kaspersky Endpoint Detection and Response Expert (cloud) auf der Open Single Management Platform (OSMP). Die Integration erfolgt durch die Programmkomponente Endpoint Detection and Response Expert (cloud) von Kaspersky Endpoint Security (im Folgenden auch *EDR Expert (cloud)* genannt).

- Kaspersky Endpoint Detection and Response und Kaspersky Network Detection and Response-Komponenten, basierend auf der Kaspersky Anti Targeted Attack Platform. Die Integration erfolgt durch die folgenden Komponenten von Kaspersky Endpoint Security:

  - Endpoint Detection and Response Expert (on-premise) (im Folgenden auch *EDR Expert (on-premise)* genannt).

  - Network Detection and Response (KATA) (im Weiteren auch *NDR (KATA)*).

- Sandbox, basierend auf der Open Single Management Platform (OSMP) oder der Kaspersky Anti Targeted Attack Platform. Die Integration erfolgt über die Komponente *Sandbox* von Kaspersky Endpoint Security.

- Kaspersky Unified Monitoring and Analysis Platform

- Kaspersky Endpoint Detection and Response Optimum Die Integration erfolgt durch Endpoint Detection and Response Optimum (im Weiteren auch *EDR Optimum*).

- Kaspersky Managed Detection and Response. Die Integration erfolgt durch Kaspersky Endpoint Security – Managed Detection and Response (im Weiteren auch *MDR*).

Integrationsfunktionen für Detection and Response-Lösungen

- Wenn Sie Kaspersky Endpoint Security im EDR-Agent-Modus verwenden, wird die Integration nur mit Kaspersky Endpoint Detection and Response Expert (on-premise) auf der Open Single Management Platform (OSMP) sowie mit den Komponenten Kaspersky Endpoint Detection and Response und Kaspersky Network Detection and Response auf der Kaspersky Anti Targeted Attack Platform unterstützt.

- Wenn Kaspersky Endpoint Security in Kaspersky Managed Detection and Response und Kaspersky Anti Targeted Attack Platform integriert ist, kann der integrierte Agent eine große Anzahl von Ereignissen im systemd-journald-Protokoll aufzeichnen. Wenn Sie die Protokollierung von Audit-Ereignissen im systemd-journald-Protokoll deaktivieren möchten, deaktivieren Sie den Socket systemd-journald-audit und starten Sie das Betriebssystem neu.

  systemd-journald-audit-Socket deaktivieren

  ```
  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.

- Detection and Response-Lösungen funktionieren möglicherweise nicht ordnungsgemäß auf virtuellen Maschinen, die aus einem Image erstellt wurden, auf dem Kaspersky Endpoint Security für Linux installiert ist. Bei der Integration mit Detection and Response-Lösungen wird eine eindeutige ID (Sensor ID) des Computers verwendet. Das Programm generiert diese ID im Rahmen der Erstinstallation, und sie bleibt auch nach der Deinstallation des Programms erhalten. Beim Klonen eines Images übernimmt die virtuelle Maschine die Sensor ID, was dazu führen kann, dass Detection and Response-Lösungen mehrere virtuelle Maschinen als dasselbe Gerät identifizieren.

  Empfehlungen zum Erstellen eines Referenzabbilds für die korrekte Integration mit MDR

  So bereiten Sie ein Referenzabbild für die korrekte Integration mit EDR Expert (on-premises) vor

Reaktionsaktionen

Bei einer Integration mit Detection and Response-Lösungen kann Kaspersky Endpoint Security Reaktionsmaßnahmen ausführen, um Sicherheitsfunktionen bereitzustellen. Detection and Response-Lösungen können Reaktionsmaßnahmen generieren und diese auf Geräten mit Kaspersky Endpoint Security automatisch ausführen. Voraussetzung dafür ist, dass diese Funktion in den Einstellungen der Detection and Response-Lösung aktiviert ist. Sie können Reaktionsmaßnahmen auch manuell anpassen und ausführen.

Die Parameter der Reaktionsmaßnahmen variieren je nach Detection and Response-Lösung, mit der Kaspersky Endpoint Security integriert ist.

Kaspersky Endpoint Security kann die folgenden Reaktionsmaßnahmen ausführen:

- Netzwerkisolation des Geräts:

Bei der Integration mit Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response Expert (cloud), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response wird die Netzwerkisolation seitens der Detection and Response-Lösung aktiviert oder deaktiviert. Sie können die Netzwerkisolation eines Geräts manuell deaktivieren.

Bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum kann ein Gerät automatisch oder manuell vom Netzwerk isoliert werden. Sie können die Parameter der Netzwerkisolation konfigurieren und die Netzwerkisolation des Geräts manuell deaktivieren.

- Datei in die Quarantäne verschieben

  Die Aktion wird mittels der Aufgabe "Datei in die Quarantäne verschieben" (*Quarantine file*) ausgeführt.

  Bei der Integration mit Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response werden die Aufgaben seitens der Detection and Response-Lösung erstellt und ausgeführt.

  Bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum kann eine Datei beim Erkennen von Kompromittierungsindikatoren (IOCs) automatisch in die Quarantäne verschoben werden.

  Bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum oder Kaspersky Managed Detection and Response können Sie Dateien auch manuell in die Quarantäne verschieben.

- Datei aus der Quarantäne wiederherstellen

  Bei der Integration mit Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response Expert (cloud), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response wird die Aktion zur Reaktion auf Bedrohungen seitens der Detection and Response-Lösung generiert. Mittels Kaspersky Security Center oder in der Befehlszeile können Sie die Aktion auch manuell ausführen.

  Bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie die Aktion manuell mittels Kaspersky Security Center oder über die Befehlszeile ausführen.

- Datei aus der Quarantäne löschen

  Bei der Integration mit Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response Expert (cloud), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response wird die Aktion zur Reaktion auf Bedrohungen seitens der Detection and Response-Lösung generiert. Mittels Kaspersky Security Center oder in der Befehlszeile können Sie die Aktion auch manuell ausführen.

  Bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie die Aktion manuell mittels Kaspersky Security Center oder über die Befehlszeile ausführen.

- Datei aus der Quarantäne abrufen

  Bei der Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response Expert (cloud) oder mit Kaspersky Endpoint Detection and Response (KATA) wird die Aktion zur Reaktion auf Bedrohungen seitens der Detection and Response-Lösung generiert.

  Bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie die Aktion manuell mittels Kaspersky Security Center ausführen.

- Datei von Gerät abrufen

  Die Aktion wird mithilfe der Aufgabe "Datei von Gerät abrufen" ausgeführt (*Get file*). Beispielsweise können Sie das Abrufen einer Ereignisprotokoll-Datei konfigurieren, die von der Anwendung eines Drittanbieters generiert wird.

  Bei der Integration mit Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response werden die Aufgaben seitens der Detection and Response-Lösung erstellt und ausgeführt.

  Bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie die Aufgaben zum Abrufen von Dateien von Geräten in der Web Console konfigurieren.

- Datei von Gerät löschen

  Die Aktion wird mithilfe der Aufgabe "Datei von Gerät löschen" ausgeführt (*Delete file*).

  Bei der Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response Expert (cloud) oder mit Kaspersky Endpoint Detection and Response (KATA) wird die Aufgabe seitens der Detection and Response-Lösung erstellt und ausgeführt.

  Bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie die Aufgaben zum Löschen von Dateien von Geräten in der Web Console konfigurieren.

- Remote-Starten eines Prozesses auf einem Gerät

  Die Aktion wird mithilfe der Aufgabe "Starten eines Prozesses" ausgeführt (*Run application*). Sie können beispielsweise per Fernzugriff ein Tool starten, das eine Gerätekonfigurationsdatei erstellt, und diese Datei anschließend mittels der Aufgabe *Datei von Gerät abrufen*.

  Bei der Integration mit Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response werden die Aufgaben seitens der Detection and Response-Lösung erstellt und ausgeführt.

  Bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie die Aufgaben zum Starten eines Prozesses in der Web Console erstellen und ausführen.

- Remote-Beenden eines Prozesses auf einem Gerät

  Die Aktion wird mithilfe der Aufgabe zum Beenden eines Prozesses ausgeführt (*Kill process*). Sie können beispielsweise remote ein Tool zur Messung der Internet-Geschwindigkeitstest beenden, welches vorher mit der Aufgabe "Prozess starten" gestartet wurde.

  Bei der Integration mit Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response werden die Aufgaben seitens der Detection and Response-Lösung erstellt und ausgeführt.

  Bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie die Aufgaben zum Beenden eines Prozesses in der Web Console erstellen und ausführen.

- Erkennung von Kompromittierungsindikatoren (IOC) auf Geräten.

  Ein *Kompromittierungsindikator (Indicator of Compromise, IOC)* bezeichnet eine Menge von Informationen über ein Objekt oder eine Aktivität, die auf einen unbefugten Zugriff auf ein Gerät hinweist (Kompromittierung der Daten). So kann beispielsweise eine hohe Anzahl an fehlgeschlagenen Anmeldeversuchen ein Indikator für eine Kompromittierung kann sein.

- Starten einer *YARA-Untersuchung*.

  Bei einer *YARA-Untersuchung* verwendet Kaspersky Endpoint Security sogenannte YARA-Dateien, um auf einem Gerät nach Signaturen schädlicher Aktivitäten zu suchen. *YARA-Dateien* sind Dateien mit YARA- oder YAR-Erweiterung, in denen YARA-Regeln enthalten sind. *YARA-Regeln* beschreiben Signaturen für gezielte Angriffe und Versuche, in die IT-Infrastruktur einer Organisation einzudringen. Kaspersky Endpoint Security untersucht Objekte anhand dieser Regeln. Wenn eine Regel erfüllt wird, meldet der Analysator eine Infektion mit entsprechenden Details im Protokoll. Die Untersuchung wird auf lokalen Laufwerken rekursiv durchgeführt. Die Untersuchung von Netzwerk-, verbundenen und Cloud-Ressourcen wird nicht unterstützt.

  Der Befehl für eine YARA-Untersuchung auf einem Kaspersky Endpoint Security-Gerät wird seitens der Lösungen Kaspersky Endpoint Detection and Response Expert (on-premise) und Kaspersky Endpoint Detection and Response Expert (cloud) erstellt und ausgeführt.

- Ausführungsprävention

- Forensische Sammlung.

  Bei der Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) und Kaspersky Endpoint Detection and Response Expert (cloud) können Sie digitale Daten erfassen, die bei der Untersuchung von Vorfällen im Zusammenhang mit Cyberkriminalität und Datenlecks nützlich sein können.

Die Aktion wird mithilfe der folgenden Aufgaben durchgeführt:

- Aufgabe zur Sammlung von forensischen Daten (*Get forensics*), welche die folgenden Arten von Informationen sammelt:
  - eine Liste mit Dateien
  - eine Liste mit Prozessen
  - eine Liste mit Mount-Punkten
- Aufgabe zum Anlegen eines Speicher-Dumps (*Get memory dump*)
- Aufgabe zum Anlegen eines Prozess-Speicher-Dumps (*Get process memory dump*)
- Aufgabe zum Erstellen eines Festplatten-Images (*Get disk image*)

Aufgaben werden seitens der Lösungen Kaspersky Endpoint Detection and Response Expert (on-premise) und Kaspersky Endpoint Detection and Response Expert (cloud) erstellt und ausgeführt.

IOC-Untersuchung

Ein *Kompromittierungsindikator (IOC)* ist ein Datensatz, der sich auf ein Objekt oder eine Aktivität bezieht und der auf unbefugten Zugriff auf den Computer (Kompromittierung von Daten) hinweist. So kann beispielsweise eine hohe Anzahl an fehlgeschlagenen Anmeldeversuchen ein Indikator für eine Kompromittierung kann sein. Mithilfe der Aufgabe *IOC-Untersuchung* können Kompromittierungsindikatoren auf dem Computer gefunden und Maßnahmen zur Reaktion auf Bedrohungen ergreifen werden.

Die IOC-Untersuchung steht in Kaspersky Endpoint Security zur Verfügung, wenn eine der folgenden Bedingungen erfüllt ist:

- Die Integration der Anwendung "Kaspersky Endpoint Security" mit der Lösung "Kaspersky Endpoint Detection and Response Optimum" ist aktiviert und die Komponente "EDR Optimum" ist aktiviert.

  In diesem Fall wird die IOC-Suche mithilfe der Aufgabe *IOC-Untersuchung* ausgeführt.

- Die Integration des Programms Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit der Komponente Kaspersky Endpoint Detection and Response (KATA) ist aktiviert, und die Komponente EDR Expert (on-premise) ist aktiviert.

  In diesem Fall wird die IOC-Untersuchung auf Seiten der entsprechenden Lösung ausgeführt.

Wenn die Aufgabe IOC-Untersuchung ausgeführt wird, erfolgt die Prüfung anhand von IOC-Bewertungen (Eigenschaften eines IOC-Objekts, z. B. Hash einer Datei) nur im Hauptnamensraum des Betriebssystems. Die Aufgabe *IOC-Untersuchung* berechnet keine Hashes für Dateien, die größer als 200 MB sind.

Um nach Anzeichen einer Kompromittierung zu suchen, verwendet Kaspersky Endpoint Security IOC-Dateien, die vom Benutzer erstellt werden müssen. Wenn Sie einen Kompromittierungsindikator manuell hinzufügen möchten, machen Sie sich bitte mit den Anforderungen an IOC-Dateien vertraut. Wenn die IOC-Datei nicht den Anforderungen entspricht, kann sie von der Anwendung nicht verwendet werden.

Die IDs aller IOC-Dateien, die innerhalb einer IOC-Suchaufgabe verwendet werden, müssen eindeutig sein. Wenn Sie mehrere IOC-Dateien mit denselben IDs laden, verwendet die Anwendung nur eine dieser IOC-Dateien. Die restlichen IOC-Dateien werden automatisch ausgeschlossen.

Aufgabe IOC-Untersuchung erstellen

Sie können Aufgaben des Typs *IOC-Untersuchung* manuell erstellen:

- In den Alarm-Details (nur für „EDR Optimum“).

  Alarm-Details ist ein Tool, mit dem alle über eine erkannte Bedrohung gesammelten Informationen angezeigt werden können. Zu den Alarm-Details gehört beispielsweise der Verlauf der auf dem Computer angezeigten Dateien. Einzelheiten zur Verwaltung der Alarm-Details finden Sie in der Hilfe zu „Kaspersky Endpoint Detection and Response Optimum“ und in der Hilfe zu „Kaspersky Endpoint Detection and Response Expert“.

- Mithilfe des Assistenten für das Erstellen einer Aufgabe.

- Lokal über die Befehlszeile.

So erstellen Sie eine IOC-Untersuchung-Aufgabe in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Linux 12.5**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **IOC-Untersuchung**.

   c. Geben Sie im Feld **Aufgabenname** einen Namen für die neue Aufgabe ein.

   d. Wählen Sie unter **Geräte, denen die Aufgabe zugewiesen wird** aus, wie Sie einen Gültigkeitsbereich für die Aufgabe festlegen möchten.

4. Wählen Sie die Geräte entsprechend Ihrer bevorzugten Methode zum Festlegen des Aufgabenbereichs aus. Wechseln Sie zum nächsten Schritt.

5. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

6. Klicken Sie auf die neue Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

7. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

8. Wechseln Sie zum Abschnitt **Bedrohungsuntersuchung**.

9. Laden Sie die IOC-Dateien hoch, um nach Kompromittierungsindikatoren zu suchen.

Nachdem Sie die IOC-Dateien hochgeladen haben, zeigt das Programm eine Übersicht über die Datei an. Dazu gehört auch eine Liste der Indikatoren, die die Überprüfung nicht bestanden haben. Nachdem Sie IOC-Dateien hochgeladen haben, können Sie die Dateien im integrierten Editor direkt in den Aufgabeneigenschaften manuell bearbeiten. Kaspersky Endpoint Security unterstützt die Bearbeitung von IOC-Dateien, die dem OpenIOC 1.1-Standard entsprechen. Der Inhalt von IOC-Dateien, die der OpenIOC Version 1.0 entsprechen, kann nicht geändert werden.

Kaspersky Endpoint Security fügt IOC-Dateien zu der IOC-Sammlung hinzu. Bei Bedarf können Sie IOC-Dateien vorübergehend aus dem Aufgabenbereich ausschließen.

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.

10. Wechseln Sie zum Abschnitt **Untersuchungseinstellungen**.

11. Konfigurieren Sie bei Bedarf die retrospektive IOC-Untersuchung.

    Die *retrospektive IOC-Untersuchung* ist ein Modus der Aufgabe *IOC-Untersuchung*. Dabei sucht Kaspersky Endpoint Security innerhalb eines bestimmten Zeitraums nach Kompromittierungsindikatoren. Dieser Modus ist für die Suche nach Kompromittierungsindikatoren anhand der Telemetrie des geschützten Computers vorgesehen (z. B. Netzwerkaktivität, Prozesse, Dateien und andere Telemetriedaten). Kaspersky Endpoint Security analysiert Daten aus den Protokollen des Betriebssystems und des Browsers auf dem Computer. Bei der retrospektiven IOC-Untersuchung werden die Protokolle der folgenden Browser analysiert: Google Chrome, Mozilla Firefox, Microsoft Edge (Version 79 oder höher).

    a. Wechseln Sie unter **Retrospektive IOC-Untersuchung** zu den Sucheinstellungen.

    b. Aktivieren Sie den Umschalter **Retrospektive IOC-Untersuchung**.

    c. Legen Sie das Zeitintervall für retrospektive IOC-Untersuchungen fest.

12. Wählen Sie die Datentypen (IOC-Dokumente) aus, die im Rahmen der Aufgabe analysiert werden sollen.

    Kaspersky Endpoint Security wählt automatisch Datentypen (IOC-Dokumente) für die Aufgabe *IOC-Untersuchung* aus, wobei der Inhalt der geladenen IOC-Dateien berücksichtigt wird. Es wird nicht empfohlen, die Auswahl von Datentypen aufzuheben.

    Darüber hinaus können Sie die Suchbereiche für den Datentyp **Dateien – FileItem** konfigurieren. Legen Sie einen IOC-Scanbereich auf dem Computer über voreingestellte Bereiche fest.

13. Wechseln Sie zum Abschnitt **Reaktionseinstellungen**.

14. Wählen Sie den Ausführungsmodus der Aufgabe aus: **Nur Alarm auslösen** oder **Alarm auslösen und reagieren**.

15. Wählen Sie eine Reaktion für den Fall aus, dass ein IOC erkannt wird:

    - **Untersuchung wichtiger Bereiche ausführen**. Wenn diese Option ausgewählt ist, führt Kaspersky Endpoint Security die *Untersuchung wichtiger Bereiche* aus. Standardmäßig überprüft Kaspersky Endpoint Security den Kernel-Speicher, die gestarteten Prozesse und die Bootsektoren.

Von Kaspersky Endpoint Security untersuchte wichtige Bereiche

- /lib/systemd
- /lib/udev
- /lib/dbus-1.0
- /usr/local/lib/systemd/user
- /usr/share/dbus-1
- /usr/share/gdm/autostart
- /usr/share/gnome/autostart
- /var/spool/at
- /var/spool/at/spool
- /var/spool/anacron
- /var/spool/cron
- /boot
- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession

- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

- **Kopie in die Quarantäne verschieben, Objekt löschen**. Wenn diese Option ausgewählt ist, löscht Kaspersky Endpoint Security das auf dem Computer gefundene schädliche Objekt. Bevor das Objekt gelöscht wird, erstellt Kaspersky Endpoint Security ein Backup davon für den Fall, dass Sie das Objekt später wiederherstellen möchten. Kaspersky Endpoint Security verschiebt die Backup-Kopie in die Quarantäne.

  Wenn dieses Kontrollkästchen deaktiviert ist, können Sie die Datei manuell in die Quarantäne verschieben, nachdem Sie die Aufgabe manuell ausgeführt haben. Wenn von der Aufgabe *IOC-Untersuchung* eine Datei gefunden wird, die Daten kompromittieren kann, können Sie diese Datei direkt über die IOC-Untersuchungsergebnisse in die Quarantäne verschieben (**Anwendungseinstellungen → IOC-Untersuchungsergebnisse**). Daraufhin startet Kaspersky Endpoint Security den Assistenten für neue Aufgaben und füllt die Daten der gefundenen Datei automatisch aus. Sie müssen nur die zusätzlichen Aufgabeneinstellungen verwalten, z. B. einen Aufgabenzeitplan einrichten.

- **Gerät vom Netzwerk isolieren**. Wenn diese Option ausgewählt ist, isoliert Kaspersky Endpoint Security den Computer vom Netzwerk, um eine Ausbreitung der Bedrohung zu verhindern. Die Isolationsdauer können Sie in den Einstellungen der Komponente „Endpoint Detection and Response“ anpassen.

  Wenn dieses Kontrollkästchen deaktiviert ist, können Sie den Computer vom Netzwerk isolieren, nachdem Sie die Aufgabe manuell ausgeführt haben. Wenn von der Aufgabe *IOC-Untersuchung* eine Datei gefunden wird, die Daten kompromittieren kann, können Sie diese Datei direkt über die IOC-Untersuchungsergebnisse in die Quarantäne verschieben (**Anwendungseinstellungen → IOC-Untersuchungsergebnisse**). Daraufhin startet Kaspersky Endpoint Security den Assistenten für neue Aufgaben und füllt die Daten der gefundenen Datei automatisch aus. Sie müssen nur die zusätzlichen Aufgabeneinstellungen verwalten, z. B. einen Aufgabenzeitplan einrichten.

16. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Zeitplan** aus.
17. Passen Sie den Zeitplan für die Aufgabe an.

    Wake-on-LAN ist für diese Aufgabe nicht verfügbar. Stellen Sie sicher, dass der Computer eingeschaltet ist, damit die Aufgabe ausgeführt werden kann.

18. Speichern Sie die vorgenommenen Änderungen.
19. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.
20. Klicken Sie auf **Starten**.

Das Ergebnis der Aufgabe *IOC-Untersuchung* können Sie in den Aufgabeneigenschaften in der Web Console unter **IOC-Untersuchungsergebnisse** einsehen. Die Aufbewahrungsdauer der Ergebnisse der IOC-Untersuchung beträgt 30 Tage. Danach beginnt Kaspersky Endpoint Security automatisch mit der Löschung alter Einträge.

So erstellen Sie die Aufgabe IOC-Untersuchung über die Befehlszeile

Führen Sie den Befehl aus:

```
kesl-control [-T] --scan-ioc --path <path to the directory or file> [--process on|off] [--hint <regular
expression>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives
```

```
all|system|critical|custom] [--excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

Symbole

Einstellungen der Aufgabe zur Schadsoftware-Untersuchung

Parameter	Description
`--path`	Pfad zu einer IOC-Datei oder einem Verzeichnis mit IOC-Dateien mit der Erweiterung .IOC oder .XML, die für die Untersuchung verwendet werden sollen. *IOC-Dateien* sind Dateien, die Sätze von Indikatoren enthalten, mit denen die Anwendung nach Übereinstimmungen sucht. IOC-Dateien müssen dem OpenIOC-Standard entsprechen. Sie können mehrere, durch Leerzeichen getrennte Pfade angeben. Sie können auch beide Arten von Pfaden (Datei und Verzeichnis) angeben.
`--process`	Analysieren der Prozessdaten, während die IOC-Untersuchung ausgeführt wird (ProcessItem-Ausdruck). Wenn der Wert des Arguments `off` ist, analysiert Kaspersky Endpoint Security die auf dem Computer ausgeführten Prozesse während der Untersuchung nicht. Falls die IOC-Datei IOC-Bedingungen des ProcessItem-IOC-Dokuments enthält, werden sie ignoriert (als Nicht-Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security die Prozessdaten nur dann, wenn das ProcessItem-IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird.
`--hint`	Analyse von Dateidaten, während die IOC-Untersuchung ausgeführt wird (Ausdrücke ProcessItem und FileItem). Für die Auswahl einer Datei bestehen folgenden Möglichkeiten: • `<full path to the executable file of the process>` – Ausdruck ProcessItem • `<full path to the file>` – Ausdruck FileItem
`--arpentry`	Analysieren von Daten über Einträge in der ARP-Tabelle, während die IOC-Untersuchung ausgeführt wird (ArpEntryItem-Begriff). Wenn der Wert des Arguments `off` ist, untersucht Kaspersky Endpoint Security die ARP-Tabelle nicht. Wenn die IOC-Datei Ausdrücke des ArpEntryItem-IOC-Dokuments enthält, werden diese ignoriert (nicht als Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security die ARP-Tabelle nur dann, wenn das ArpEntryItem-IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird.
`--ports`	Analysieren von Daten über Ports, die während der IOC-Untersuchung zum Abhören geöffnet sind (PortItem-Ausdruck). Wenn der Wert des Arguments `off` ist, untersucht Kaspersky Endpoint Security die Tabelle der auf dem Gerät aktiven Verbindungen nicht. Wenn die IOC-Datei Ausdrücke des PortItem-IOC-Dokuments enthält, werden diese ignoriert (nicht als Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security die Tabelle der aktiven Verbindungen nur dann, wenn das PortItem-IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird.
`--system`	Analysieren von Umgebungsdaten, während die IOC-Untersuchung ausgeführt wird (SystemInfoItem-Ausdruck). Wenn der Wert des Arguments `off` ist, analysiert Kaspersky Endpoint Security die Umgebungsdaten nicht. Wenn die IOC-Datei Ausdrücke des SystemInfoItem-IOC-Dokuments enthält, werden diese ignoriert (nicht als Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security die Umgebungsdaten nur dann, wenn das SystemInfoItem-IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird.
`--files`	Analysieren von Dateidaten, während die IOC-Untersuchung ausgeführt wird (FileItem-Ausdruck). Wenn der Wert des Arguments `off` ist, analysiert Kaspersky Endpoint Security die Dateidaten nicht. Wenn die IOC-Datei Ausdrücke des FileItem-IOC-Dokuments enthält, werden diese ignoriert (nicht als Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security die Dateidaten nur dann, wenn das FileItem-IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird.
`--drives`	Festlegen des IOC-Untersuchungsbereichs, wenn Daten für das FileItem-IOC-Dokument analysiert werden. Für den Untersuchungsbereich können Sie die folgenden Werte festlegen: • `<all>` für alle verfügbaren Dateibereiche. • `<system>` für Dateien in Ordnern, in denen das Betriebssystem installiert ist. • `<critical>` für temporäre Dateien in Benutzer- und Systemordnern. • `<custom>` für Dateien in benutzerdefinierten Bereichen (`/scope=<list of folders to scan>`). Ist das Argument nicht angegeben, so wird die Untersuchung für kritische Bereiche durchgeführt.
`--excludes`	Festlegen des IOC-Ausnahmebereichs, wenn Daten für das FileItem-IOC-Dokument analysiert werden. Sie können mehrere durch Leerzeichen getrennte Pfade angeben.
`--scope`	Benutzerdefinierter IOC-Untersuchungsbereich, wenn Daten für das IOC-Dokument FileItem analysiert werden (`/drives=custom`). Sie können mehrere durch Leerzeichen getrennte Pfade angeben.

Parameter	Description
`--action`	Aktion, die ausgeführt wird, wenn Kompromittierungsindikatoren erkannt werden: • `Skip`. Wenn diese Option ausgewählt ist, erkennt Kaspersky Endpoint Security nur Dateien, die zu einer Kompromittierung von Daten führen können. • `QuarantineFile`. Wenn diese Option ausgewählt ist, löscht Kaspersky Endpoint Security das auf dem Computer gefundene schädliche Objekt. Bevor das Objekt gelöscht wird, erstellt Kaspersky Endpoint Security ein Backup davon für den Fall, dass Sie das Objekt später wiederherstellen möchten. Kaspersky Endpoint Security verschiebt die Backup-Kopie in die Quarantäne. • `IsolateHost`. Wenn diese Option ausgewählt ist, isoliert Kaspersky Endpoint Security den Computer vom Netzwerk, um eine Ausbreitung der Bedrohung zu verhindern. • `ScanCriticalAreas`. Wenn diese Option ausgewählt ist, führt Kaspersky Endpoint Security die *Untersuchung wichtiger Bereiche* aus. Standardmäßig überprüft Kaspersky Endpoint Security den Kernel-Speicher, die gestarteten Prozesse und die Bootsektoren.

Netzwerkisolation

Bei einer Integration mit Detection and Response-Lösungen kann ein Gerät im Rahmen einer Reaktionsmaßnahme auf eine Bedrohung vom Netzwerk isoliert werden.

Besonderheiten bei Ausführung der Netzwerkisolation

Sobald die Netzwerkisolation aktiviert ist, unterbricht die Anwendung 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 Security Center Administrationsagent initiiert werden.
- Verbindungen mit SVMs und Integrationsserver, wenn die App im Light Agent-Modus verwendet wird.
- Verbindungen zu KSN (bei Integration mit Kaspersky Managed Detection and Response).

Die Netzwerkisolation kann angewendet werden, wenn eine der folgenden Bedingungen erfüllt ist:

- Die Integration der Anwendung "Kaspersky Endpoint Security" mit der Lösung "Kaspersky Endpoint Detection and Response Optimum" ist aktiviert und die Komponente "EDR Optimum" ist aktiviert.
- Die Integration des Programms Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit der Komponente Kaspersky Endpoint Detection and Response (KATA) ist aktiviert, und die Komponente EDR Expert (on-premise) ist aktiviert.
- Die Integration der Anwendung "Kaspersky Endpoint Security" mit der Lösung "Kaspersky Managed Detection and Response" ist aktiviert und die MDR-Komponente ist aktiviert.

Bei der Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise), Kaspersky Endpoint Detection and Response (KATA) und Kaspersky Managed Detection and Response wird die Netzwerkisolation eines Geräts auf Seiten der Detection and Response-Lösung aktiviert oder deaktiviert, und Ausnahmen für die Netzwerkisolation werden konfiguriert. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premise), in der Hilfe zu Kaspersky Anti Targeted Attack Platform oder in der Hilfe zu Kaspersky Managed Detection and Response. Bei Bedarf können Sie die Netzwerkisolation eines Geräts manuell deaktivieren:

- In den Geräteeigenschaften in der Web Console (nur bei Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA))
- Über die Befehlszeile

Das manuelle Deaktivieren der Netzwerkisolation ist unabhängig davon möglich, ob die Integration mit Detection and Response-Lösungen aktiviert ist und ob das Gerät durch eine Richtlinie abgedeckt ist.

Bei Integration mit Kaspersky Endpoint Detection and Response Optimum kann die Netzwerkisolation in einem der folgenden Modi angewendet werden:

- Automatischer Modus der Netzwerkisolation. Das Gerät kann aufgrund der Erkennung eines Kompromittierungsindikators (IOC) automatisch vom Netzwerk isoliert werden. Wenn Sie beim Erstellen und Konfigurieren der Aufgabenparameter für die *IOC-Untersuchung* im Block **Aktionen beim Erkennen von IOCs** die Kontrollkästchen **Bei Erkennung eines IOCs folgende Reaktion anwenden** und **Gerät vom Netzwerk isolieren** aktivieren, wird die Netzwerkisolation automatisch aktiviert, sobald die Anwendung Kompromittierungsindikatoren erkennt.

  Im automatischen Modus können Sie die folgenden Parameter der Netzwerkisolation konfigurieren:

  - Den Zeitraum ändern, nach dem die Netzwerkisolation automatisch deaktiviert wird.
  - Für automatisch isolierte Geräte Ausnahmen aus der Netzwerkisolation konfigurieren.

  > Wenn ein automatisch isoliertes Gerät von einer Richtlinie abgedeckt wird, werden die in der Richtlinie angegebenen Einstellungen angewendet. Wenn keine Richtlinie angewendet wird, werden die in den Geräteeigenschaften angegebenen Parameter angewendet.

- Manueller Modus der Netzwerkisolation. Das Gerät kann vom Netzwerk isoliert werden, während die erkannte Bedrohung untersucht wird. Sie können die Netzwerkisolation für ein Gerät manuell im Fenster mit den Alarm-Details sowie in den Geräteeigenschaften in der Web Console aktivieren.

  Im manuellen Modus können Sie die folgenden Parameter der Netzwerkisolation konfigurieren:

  - Den Zeitraum ändern, nach dem die Netzwerkisolation automatisch deaktiviert wird.
  - Für manuell isolierte Geräte Ausnahmen aus der Netzwerkisolation konfigurieren.

Bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie die Netzwerkisolation eines Geräts in den Geräteeigenschaften in der Web Console und über die Befehlszeile manuell deaktivieren.

Den Status der Netzwerkisolation des Geräts können Sie über die Befehlszeile überprüfen.

Ein isoliertes Gerät bekommt 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.

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., die App wird nicht ausgeführt) ist die Blockierung des Datenverkehrs bei aktivierter Netzwerkisolation durch Detection and Response nicht garantiert.

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.

Proxyserver werden nicht automatisch zu den Ausnahmen für die Netzwerkisolation hinzugefügt. Damit Kaspersky Endpoint Security die Verbindung zum Server, der die Integration gewährleistet, nicht verliert, müssen Sie daher einen Proxyserver manuell zu den Ausnahmen hinzufügen.

Um Prozesse nach Namen aus der Netzwerkisolation auszuschließen, sind Geräte mit Kernelversion ab 4.18 mit Unterstützung für eBPF mit BTF und mit aktivierten tracepoints-Funktionen und kprobes für das Kernel-Tracing erforderlich.

Wenn Kaspersky Endpoint Security im Standard-Modus oder im EDR-Agent-Modus verwendet wird, empfehlen wir bei Verwendung der Netzwerkisolation Folgendes:

- Verwendung des KSN-Proxyservers, um mit Kaspersky Security Network zu interagieren.
- Verwendung von Kaspersky Security Center als Proxyserver, um die Anwendung zu aktivieren.

  Wenn es nicht möglich ist, Kaspersky Security Center als Proxyserver zu verwenden, müssen die erforderlichen Parameter des Proxyservers konfiguriert und dieser zu den Ausnahmen hinzugefügt werden.
- Verwendung von Kaspersky Security Center als Quelle für die Datenbankaktualisierungen.

Diese Empfehlungen gelten nicht, wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird.

Netzwerkisolation eines Geräts manuell in der Web Console aktivieren und deaktivieren

Sie können die Netzwerkisolierung eines Geräts nur bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum anhand der Web Console aktivieren.

Manuelles Aktivieren oder Deaktivieren der Netzwerkisolation eines Geräts bei Integration mit Kaspersky Endpoint Detection and Response Optimum

So aktivieren oder deaktivieren Sie für ein Gerät die Netzwerkisolation manuell:

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

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie bei Bedarf eine Administrationsgruppe aus, suchen Sie Ihr Gerät und klicken Sie auf dessen Namen.

3. Wechseln Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts zur Registerkarte **Anwendungen**.

4. Klicken Sie in der Liste der auf dem Gerät installierten Anwendungen auf den Namen der Anwendung Kaspersky Endpoint Security.

5. Wählen Sie im nächsten Fenster mit den Anwendungseigenschaften auf der Registerkarte **Anwendungseinstellungen** den Abschnitt **Integrierte Agenten** → **Endpoint Detection and Response** aus.

6. Führen Sie im neuen Fenster im Block mit den Einstellungen für die **Netzwerkisolation** einen der folgenden Schritte aus:

   - Klicken Sie auf die Schaltfläche **Gerät vom Netzwerk isolieren**, um die Netzwerkisolation eines Geräts zu aktivieren. Die Schaltfläche ist nur verfügbar, wenn der Umschalter **Endpoint Detection and Response** aktiviert ist.

     Wenn Sie auf diese Schaltfläche klicken, wird das Gerät für die in den Eigenschaften der Aufgabe *Netzwerkisolation aktivieren (NetworkIsolationStart)* angegebene Dauer isoliert.

   - Klicken Sie auf die Schaltfläche **Isoliertes Gerät freigeben**, um die Netzwerkisolierung des Geräts zu deaktivieren. Die Schaltfläche ist unabhängig davon verfügbar, ob der Umschalter **Endpoint Detection and Response** aktiviert oder deaktiviert ist.

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

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.

Manuelles Deaktivieren der Netzwerkisolation eines Geräts bei der Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder Kaspersky Endpoint Detection and Response (KATA)

So deaktivieren Sie für ein Gerät die Netzwerkisolation manuell:

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. 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 **Anwendungen**.

5. Klicken Sie in der Liste der auf dem Gerät installierten Anwendungen auf den Namen der Anwendung Kaspersky Endpoint Security.

6. Wählen Sie im nächsten Fenster mit den Anwendungseigenschaften auf der Registerkarte **Anwendungseinstellungen** den Abschnitt **Detection and Response** aus.

7. Klicken Sie unter **Netzwerkisolation (EDR Expert (on-premise))** auf die Schaltfläche **Isoliertes Gerät freigeben**, um die Netzwerkisolation des Geräts zu deaktivieren.

Nachdem die Netzwerkisolation eines Geräts deaktiviert wurde, entfernt Kaspersky Endpoint Security das Tag **ISOLATED FROM NETWORK** vom Gerät.

Dauer der Netzwerkisolation im automatischen Modus konfigurieren

Die Dauer der Netzwerkisolation im automatischen Modus kann nur bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum konfiguriert werden:

Die Netzwerkisolation von Geräten, die im Rahmen einer Aufgabe zur *IOC-Untersuchung* isoliert wurden, wird nach einer angegebenen Zeitspanne automatisch deaktiviert. Sie können diesen Zeitraum in der Web Console sowohl in den Geräteeigenschaften als auch in den Richtlinieneigenschaften konfigurieren. Die Parameter zur Netzwerkisolation in den Richtlinieneigenschaften der Web Console werden in Anhang 5 beschrieben. Die Einstellungen der Netzwerkisolation in den Eigenschaften des verwalteten Geräts werden in der folgenden Tabelle beschrieben.

Wenn ein Gerät von einer Richtlinie abgedeckt wird, werden die in der Richtlinie angegebenen Einstellungen angewendet und die Einstellung zur automatischen Deaktivierung der Netzwerkisolation ist in den Geräteeigenschaften nicht verfügbar. Wenn das Gerät nicht von der Richtlinie abgedeckt wird, werden die in den Geräteeigenschaften angegebenen Parameter angewendet.

Standardmäßig deaktiviert die Anwendung 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 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. 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 **Anwendungen**.

5. Klicken Sie in der Liste der auf dem Gerät installierten Anwendungen auf den Namen der Anwendung Kaspersky Endpoint Security.

6. Wählen Sie im nächsten Fenster mit den Anwendungseinstellungen auf der Registerkarte **Anwendungseinstellungen** den Abschnitt **Detection and Response** und folgen Sie dem Link **Endpoint Detection and Response Optimum**.

7. Klicken Sie im Block mit den Einstellungen der **Netzwerkisolation** auf den Link **Einrichten der Gerätefreigabe**.

8. Aktivieren Sie im neuen Fenster **Einstellung der Gerätefreigabe** das Kontrollkästchen **Automatisch isoliertes Gerät freigeben nach** und geben Sie im Feld darunter die Dauer in Stunden an, nach deren Ablauf das Gerät automatisch freigegeben wird.

9. Speichern Sie die vorgenommenen Änderungen.

Parameter der Netzwerkisolation manuell einrichten

Das manuelle Isolieren eines Geräts vom Netzwerk ist nur bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum möglich.

Wenn Sie die Netzwerkisolation eines Geräts manuell aktivieren, können Sie die Parameter der Netzwerkisolation anhand der lokalen Aufgabe *Aktivieren der Netzwerkisolation* (*NetworkIsolationStart*) vorkonfigurieren. Sie können Ausnahmen von der Netzwerkisolation und die Dauer der Netzwerkisolation für ein Gerät konfigurieren.

Die Aufgabe *Netzwerkisolation aktivieren* ist vorinstalliert und wird nur in den folgenden Fällen automatisch ausgeführt:

- Wenn Sie in den Geräteeigenschaften auf die Schaltfläche **Gerät vom Netzwerk isolieren** geklickt haben.
- Wenn Sie die Netzwerkisolation des Geräts im Fenster mit den Alarm-Details aktivieren.

Sie können weder eine neue Instanz der Aufgabe *Aktivieren der Netzwerkisolation* über die Schaltfläche **Hinzufügen** erstellen, noch sie durch Klicken auf die Schaltfläche **Ausführen** starten. Die Aufgabe ist nur in den Geräteeigenschaften verfügbar, in denen Sie deren Einstellungen ändern können, bevor Sie die Netzwerkisolation für das Gerät aktivieren.

Die Parameter der Aufgabe *Aktivieren der Netzwerkisolation* gelten unabhängig davon, ob auf das Gerät eine Richtlinie angewendet wird.

So konfigurieren Sie für ein Gerät die Parameter der Netzwerkisolation:

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. 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 **Aufgaben**.

5. Klicken Sie in der Aufgabenliste auf die Aufgabe *Aktivieren der Netzwerkisolation*.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

6. Gehen Sie zur Registerkarte **Anwendungseinstellungen**.

7. Klicken Sie auf den Link **Ausschlüsse anpassen**, um das Fenster **Ausnahmen** zu öffnen.

8. 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**.

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

10. Geben Sie im Feld **Gerät isolieren auf** die erforderliche Dauer der Netzwerkisolation in Stunden ein.

    Die Standarddauer der Netzwerkisolation beträgt 5 Stunden.

    Die zulässige Mindestdauer der Netzwerkisolation beträgt 1 Stunde betragen.

11. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Ausnahmen von der Netzwerkisolation in der Web Console konfigurieren

Wenn Kaspersky Endpoint Security in Endpoint Detection and Response Expert (on-premise), Kaspersky Endpoint Detection and Response (KATA) oder Kaspersky Managed Detection and Response integriert ist, werden Ausnahmen von der Netzwerkisolation auf der Seite der Detection and Response-Lösung konfiguriert. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premise), in der Hilfe zu Kaspersky Anti Targeted Attack Platform oder in der Hilfe zu Kaspersky Managed Detection and Response.

Bei der Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Optimum können Sie Ausnahmen von der Netzwerkisolation auf folgende Weise konfigurieren:

- In den Richtlinieneigenschaften in der Web Console. In der Richtlinie konfigurierten Ausnahmen werden bei der automatischen Netzwerkisolation der Geräte angewendet, die von der Richtlinie abgedeckt wird.

- In den Geräteeigenschaften in der Web Console. In den Geräteeigenschaften konfigurierten Ausnahmen werden bei der automatischen Netzwerkisolation der Geräte angewendet, die nicht von einer Richtlinie abgedeckt sind.

- In den Einstellungen der lokalen Aufgabe *Aktivieren der Netzwerkisolation* (*NetworkIsolationStart*). In den Eigenschaften dieser Aufgabe konfigurierten Ausnahmen werden bei manueller Aktivierung der Netzwerkisolation auf Geräte angewendet. Die Einstellungen der Aufgabe *Netzwerkisolation aktivieren* gelten unabhängig davon, ob eine Richtlinie auf das Gerät angewendet wird.

Zum Konfigurieren von Ausnahmen von der Netzwerkisolation stellt das Programm eine Liste mit *Standard-Netzwerkprofilen* bereit. Die Netzwerkprofile bestehen aus Regeln, die einen unterbrechungsfreien Betrieb von Geräten gewährleisten, denen DNS/DHCP-Server- und DNS/DHCP-Client-Rollen zugewiesen sind. Sie können die Einstellungen von Standardnetzwerkprofilen ändern und Ausnahmen manuell festlegen.

Das Hinzufügen oder Entfernen von Ausnahmen für die Netzwerkisolation ist in den Geräteeigenschaften nicht möglich, wenn das Gerät einer Richtlinie unterliegt.

So fügen Sie eine Ausnahme für die Netzwerkisolation in der Web Console hinzu

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response**.
5. Klicken Sie im Block **Netzwerkisolation** auf den Link **Ausnahmen**.
   Dadurch wird ein Fenster mit einer Liste der Ausnahmen von der Netzwerkisolation geöffnet.
6. Sie können eine Netzwerkverbindung auf folgende Weise ausschließen:
   - Klicken Sie auf **Hinzufügen** und geben Sie Informationen zur Netzwerkverbindung ein.

     Sie können ein Programm hinzufügen, für das die Komponente Netzwerkverbindungen nicht blockiert. Diese Einstellung gilt für Geräte mit Kernel-Version 4.18 oder höher mit Unterstützung für eBPF und BTF sowie mit aktivierten tracepoints- und kprobes-Funktionen für das Kernel-Tracing.

   - Klicken Sie auf die Schaltfläche **Aus Profil hinzufügen** und wählen Sie ein Netzwerkprofil aus der Liste aus.
7. Speichern Sie die vorgenommenen Änderungen.

So entfernen Sie eine Ausnahme für die Netzwerkisolation in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response**.
5. Klicken Sie im Block **Netzwerkisolation** auf den Link **Ausnahmen**.
   Dadurch wird ein Fenster mit einer Liste der Ausnahmen von der Netzwerkisolation geöffnet.
6. Aktivieren Sie das Kontrollkästchen neben der Netzwerkverbindung und klicken Sie auf **Löschen**.
7. Speichern Sie die vorgenommenen Änderungen.

Die Datei in die Quarantäne verschieben.

Kaspersky Endpoint Detection and Response kann als Reaktion auf Bedrohungen Aufgaben des Typs *Datei in Quarantäne verschieben* erstellen. Dies ist erforderlich, um die Folgen der Bedrohung zu minimieren. Die *Quarantäne* ist ein spezieller lokaler Speicher auf dem Computer. Der Benutzer kann Dateien, die er für gefährlich für den Computer hält, in die Quarantäne verschieben. Dateien in der Quarantäne werden in verschlüsselter Form gespeichert und stellen keine Gefahr für das Gerät dar.

Aufgaben des Typs *Datei in Quarantäne verschieben* werden wie folgt erstellt:

- In den Alarm-Details (nur für „EDR Optimum“).

  Alarm-Details ist ein Tool, mit dem alle über eine erkannte Bedrohung gesammelten Informationen angezeigt werden können. Zu den Alarm-Details gehört beispielsweise der Verlauf der auf dem Computer angezeigten Dateien. Sie können die zu löschende Datei direkt in den Alarm-Details auswählen. Daraufhin startet Kaspersky Endpoint Security den Assistenten für neue Aufgaben und füllt die Daten der gefundenen Datei automatisch aus. Sie müssen nur die zusätzlichen Aufgabeneinstellungen verwalten, z. B. einen Aufgabenzeitplan einrichten.

- Mithilfe des Assistenten für das Erstellen einer Aufgabe.

  Im Assistenten für das Erstellen einer Aufgabe können der Pfad zur Datei oder zum Verzeichnis und der Hash der zu löschenden Datei manuell eingegeben werden. Sie können auch zusätzliche Aufgabeneinstellungen verwalten, z. B. den Aufgabenzeitplan einrichten.

- In den Einstellungen der Aufgabe *IOC-Untersuchung*.

  Wenn von der Aufgabe *IOC-Untersuchung* eine Datei gefunden wird, die Daten kompromittieren kann, können Sie diese Datei direkt über die IOC-Untersuchungsergebnisse in die Quarantäne verschieben (**Anwendungseinstellungen** → **IOC-Untersuchungsergebnisse**). Daraufhin startet Kaspersky Endpoint Security den Assistenten für neue Aufgaben und füllt die Daten der gefundenen Datei automatisch aus. Sie müssen nur die zusätzlichen Aufgabeneinstellungen verwalten, z. B. einen Aufgabenzeitplan einrichten.

Die Datei darf maximal 100 MB groß sein.

So erstellen Sie eine Aufgabe Datei in Quarantäne verschieben

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Linux**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Datei in Quarantäne verschieben**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.

5. Beenden Sie den Assistenten durch Klick auf **Fertigstellen**.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

6. Klicken Sie auf die neue Aufgabe.

7. Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

8. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

9. Klicken Sie in der Dateiliste auf **Hinzufügen**.

   Der Assistent zum Hinzufügen von Dateien wird gestartet.

10. Um eine Datei hinzuzufügen, müssen Sie den Dateipfad oder den Verzeichnispfad und den Datei-Hash eingeben.

11. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Zeitplan** aus.

12. Passen Sie den Zeitplan für die Aufgabe an.

13. Speichern Sie die vorgenommenen Änderungen.

14. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

15. Klicken Sie auf **Starten**.

    Daraufhin verschiebt Kaspersky Endpoint Security die Datei in die Quarantäne.

Ist die Datei durch einen anderen Prozess gesperrt, so wird für die Aufgabe der Status *Completed* angezeigt, die Datei selbst wird aber erst nach dem Neustart des Computers in die Quarantäne verschoben. Bestätigen Sie nach dem Neustart des Computers, dass die Datei gelöscht werden soll.

Die Aufgabe *Datei in Quarantäne verschieben* kann mit dem Fehler *Zugriff verweigert* abschließen, wenn Sie versuchen, eine ausführbare Datei, die gerade ausgeführt wird, in die Quarantäne zu verschieben. Erstellen Sie für die Datei eine Aufgabe „Prozess beenden“ und versuchen Sie es erneut.

Die Aufgabe *Datei in Quarantäne verschieben* kann mit dem Fehler *Zu wenig Platz im Quarantäne-Speicher* abschließen, wenn Sie versuchen, eine zu große Datei in die Quarantäne zu verschieben. Löschen Sie die Quarantäne oder erhöhen Sie die Größe des Quarantäne-Speichers. Dann versuchen Sie es erneut.

Datei von Gerät abrufen

Sie können Dateien von Benutzercomputern abrufen. Beispielsweise können Sie das Abrufen einer Ereignisprotokoll-Datei konfigurieren, die von der Anwendung eines Drittanbieters generiert wird. Als Ergebnis der Ausführung der Aufgabe wird eine Kopie der Datei in der Quarantäne gespeichert. Die *Quarantäne* ist ein spezieller lokaler Speicher auf dem Computer. Sie können diese Datei mithilfe der Web Console (**Vorgänge** → **Datenverwaltung** → **Quarantäne**) aus der Quarantäne auf Ihren Computer herunterladen. Die Originaldatei auf dem Gerät des Benutzers verbleibt im Originalverzeichnis.

In Kaspersky Security Center erhalten in der Liste der Dateien in Quarantäne alle Dateien, die über die Aufgabe *Datei anfordern* abgerufen wurden, unabhängig von den Ergebnissen der Dateiuntersuchung den Status *Infiziert*.

Die Datei darf maximal 100 MB groß sein.

So erstellen Sie eine Aufgabe Datei anfordern

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Linux**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Datei anfordern**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.

5. Beenden Sie den Assistenten durch Klick auf **Fertigstellen**.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

6. Klicken Sie auf die neue Aufgabe.

7. Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

8. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

9. Klicken Sie in der Dateiliste auf **Hinzufügen**.

   Der Assistent zum Hinzufügen von Dateien wird gestartet.

10. Um eine Datei hinzuzufügen, müssen Sie den Dateipfad oder den Verzeichnispfad und den Datei-Hash eingeben.

11. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Zeitplan** aus.
12. Passen Sie den Zeitplan für die Aufgabe an.
13. Speichern Sie die vorgenommenen Änderungen.
14. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.
15. Klicken Sie auf **Starten**.

    Daraufhin erstellt Kaspersky Endpoint Security eine Kopie der Datei und verschiebt sie in die Quarantäne. Sie können die Datei über die „Web Console“ aus der Quarantäne herunterladen.

Die Aufgabe *Datei anfordern* wird mit einem Fehler beendet, wenn:

- Die angegebene Datei wurde nicht gefunden.
- Es wurden falsche Dateidaten angegeben (Dateiname oder Prüfsumme).
- Unzureichende Rechte zum Ausführen von Aktionen für die angegebene Datei.
- Die angegebene Datei ist gesperrt.
- Nicht genügend Platz in der Quarantäne.
- Die angegebene Datei ist zu groß (über 100 MB).

Datei von Gerät löschen

Sie können Dateien mithilfe der Aufgabe *Datei löschen* per Fernzugriff löschen. Sie können beispielsweise eine Datei aus der Ferne löschen, um auf Bedrohungen zu reagieren.

So erstellen Sie eine Aufgabe Datei löschen

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.
3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Linux**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Datei löschen**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.
4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.

5. Beenden Sie den Assistenten durch Klick auf **Fertigstellen**.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

6. Klicken Sie auf die neue Aufgabe.

7. Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

8. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

9. Um eine Datei hinzuzufügen, müssen Sie den Verzeichnispfad und den Datei-Hash eingeben.

10. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Zeitplan** aus.

11. Passen Sie den Zeitplan für die Aufgabe an.

12. Speichern Sie die vorgenommenen Änderungen.

13. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

14. Klicken Sie auf **Starten**.

    Daraufhin löscht Kaspersky Endpoint Security die Datei vom entsprechenden Computer. Ist die Datei durch einen anderen Prozess gesperrt, so wird für die Aufgabe der Status *Ausgeführt* angezeigt, die Datei wird aber erst nach dem Neustart des Computers gelöscht. Bestätigen Sie nach dem Neustart des Computers, dass die Datei gelöscht werden soll.

Einen Prozess starten

Sie können Dateien mithilfe der Aufgabe *Prozess-Start* per Fernzugriff ausführen. Sie können beispielsweise aus der Ferne ein Dienstprogramm ausführen, das die Computerkonfigurationsdatei erstellt. Anschließend können Sie die Aufgabe *Datei anfordern* verwenden, um die erstellte Datei in Kaspersky Security Center Web Console zu empfangen.

Wenn sich SELinux in Ihrem Betriebssystem im Modus `Enforcing` befindet, müssen Sie zum Starten der Aufgabe *Prozess-Start* eine zusätzliche Konfiguration von SELinux vornehmen.

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

Wenn Sie SELinux auf Ihrem Betriebssystem im Modus `Enforcing` verwenden möchten, müssen Sie zur Ausführung von Reaktionsaktionen bei der Integration mit Detection and Response-Lösungen zusätzlich die SELinux-Einstellungen verwalten.

Diese SELinux-Konfiguration erfordert Root-Rechte.

So konfigurieren Sie SELinux für Reaktionsaktionen:

1. Schalten Sie SELinux in den Erlaubnismodus:

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

     ```
     SELinux in den Modus „permissive“ umschalten

     setenforce Permissive
     ```

   - Wenn SELinux deaktiviert ist, legen Sie `SELINUX=permissive` in der Konfigurationsdatei /etc/selinux/config fest 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 alle Aufgaben aus, um die Reaktionsaktionen durchzuführen, die Sie im Rahmen der Integration mit Detection and Response-Lösungen verwenden möchten.

4. Stellen Sie sicher, dass die Datei audit.log keine Fehler enthält.

   ```
   Datei audit.log anzeigen

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

5. Wenn die Datei audit.log Fehler enthält, erstellen und laden Sie ein neues Regelmodul auf Basis der blockierenden Einträge, um die Fehler zu beheben. Führen Sie anschließend die Aufgaben für Reaktionsaktionen erneut aus.

   ```
   Erstellen und laden Sie ein neues Regelmodul basierend auf blockierenden Einträgen:

   grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   semodule -i kesl.pp
   ```

6. Schalten Sie SELinux in den Modus „enforcing“ um.

   ```
   setenforce Enforcing
   ```

So erstellen Sie eine Aufgabe Prozess-Start

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Linux**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Prozess-Start**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.

5. Beenden Sie den Assistenten durch Klick auf **Fertigstellen**.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

6. Klicken Sie auf die neue Aufgabe.

7. Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

8. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

9. Geben Sie den Befehl zum Starten des Prozesses ein:

   - **Ausführbarer Befehl**. Feld zur Eingabe des Befehls zum Starten des Prozesses.

     Wenn Sie beispielsweise das Dienstprogramm `klnagchk` ausführen möchten, das die Verbindung zum Administrationsserver überprüft, geben Sie `/opt/kaspersky/klnagent/bin/klnagchk` ein.

   - **Befehlszeilenargumente (optional)**. Feld zur Eingabe von Befehlszeilenargumenten, um beim Start zusätzliche Eingaben an das Skript, das Dienstprogramm oder die Anwendung zu übergeben.

     Sie können beispielsweise das Argument `-logfile /tmp/klnagchk.log` eingeben. Dieses Argument weist das Tool an, das Ergebnis in einer Datei mit dem Namen `klnagchk.log` in `/tmp` zu speichern. Wenn Sie mehrere Argumente übergeben möchten, müssen Sie diese durch ein Leerzeichen trennen.

   - **Pfad zum Arbeitsverzeichnis (optional)**. Feld zur Eingabe des Pfads zum Arbeitsverzeichnis, in dem der Prozess die Dateien ablegt.

     Beispielsweise können Sie `/tmp` eingeben und das Dienstprogramm `klnagchk` mit den folgenden Argumenten ausführen: `-logfile klnagchk.log -savecert certificate.cer`. In diesem Fall werden beide Dateien in `tmp` erstellt.

10. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Zeitplan** aus.

11. Passen Sie den Zeitplan für die Aufgabe an.

12. Speichern Sie die vorgenommenen Änderungen.

13. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

14. Klicken Sie auf **Starten**.

    Daraufhin führt Kaspersky Endpoint Security den Befehl im Hintergrund aus und startet den Prozess. Die Ergebnisse der Aufgabe können Sie in den Aufgabeneigenschaften im Abschnitt **Ausführungsergebnisse** einsehen.

Eines Prozesses beenden

Sie können Prozesse mithilfe der Aufgabe *Prozess beenden* ferngesteuert beenden. Sie können beispielsweise einen Prozess, der infolge schädlicher Aktivität gestartet wurde, remote beenden.

Wenn Sie das Ausführen einer Datei unterbinden möchten, können Sie die Ausführungsverhinderungskomponente konfigurieren. Sie können die Ausführung von ausführbaren Dateien, Skripten und Dateien im Office-Format verbieten.

So erstellen Sie die Aufgabe Prozess beenden

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Linux**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option *Prozess beenden*.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.

5. Beenden Sie den Assistenten durch Klick auf **Fertigstellen**.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

6. Klicken Sie auf die neue Aufgabe.

7. Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

8. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

9. Um den Prozess zu beenden, müssen Sie die Datei des Prozesses auswählen, den Sie beenden möchten. Für die Auswahl einer Datei bestehen folgenden Möglichkeiten:

   - Geben Sie den vollständigen Namen der Datei ein.
   - Geben Sie den Datei-Hash und den Dateipfad ein.
   - Geben Sie die PID des Prozesses ein (nur für lokale Aufgaben).
   - Wenn sich die Datei auf einem Netzlaufwerk befindet, geben Sie vor dem Dateipfad die Zeichen `\\` ein, nicht den Laufwerksbuchstaben. Beispiel: `\\server\shared_folder\file.exe`. Wenn der Dateipfad einen Netzlaufwerksbuchstaben enthält, erhalten Sie möglicherweise den Fehler *Datei wurde nicht gefunden*.

10. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Zeitplan** aus.

11. Passen Sie den Zeitplan für die Aufgabe an.

12. Speichern Sie die vorgenommenen Änderungen.

13. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

14. Klicken Sie auf **Starten**.

    Daraufhin löscht Kaspersky Endpoint Security den Prozess vom entsprechenden Computer. Die Ergebnisse der Aufgabe können Sie in den Aufgabeneigenschaften im Abschnitt **Ergebnisse** einsehen.

Ausführungsprävention für Objekte

Sie können diese Reaktionsaktion bei der Integration mit Kaspersky Detection and Response-Lösungen anwenden, von denen Kaspersky Endpoint Security Regeln zur Ausführungsprävention erhält.

Wenn ein Objekt einer Regel entspricht, verhindert Kaspersky Endpoint Security die Ausführung dieses Objekts.

Ausführungsprävention für Objekte EDR Expert (on-premise)

Bei der Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise), Kaspersky Endpoint Detection and Response Expert (cloud) oder Kaspersky Endpoint Detection and Response (KATA) können Sie in der Konsole der entsprechenden Lösung Regeln konfigurieren, um die Ausführung von Objekten zu blockieren.

Wenn die Integration mit der Lösung Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit der Komponente Kaspersky Endpoint Detection and Response (KATA) aktiviert ist, können Sie die Ausführungsprävention für Objekte in den Richtlinieneigenschaften (**Programmeinstellungen → Konfiguration der integrierten Agenten → Endpoint Detection and Response Expert (On-Premises)**) aktivieren oder deaktivieren.

Um die Ausführungsprävention für Objekte zu aktivieren, setzen Sie den Umschalter auf **Ausführungsprävention AKTIVIERT**.

Ausführungsprävention für Objekte (EDR Optimum)

Bei der Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie die Ausführungsprävention für Objekte und Regeln zur Ausführungsprävention in der Web Console konfigurieren.

So aktivieren Sie die Ausführungsprävention für Objekte in einer Kaspersky Security Center-Richtlinie

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Konfiguration der integrierten Agenten → Endpoint Detection and Response**.

5. Gehen Sie zur Registerkarte **Ausführungsprävention**.

6. Stellen Sie den Umschalter auf **Ausführungsprävention AKTIVIERT**.

7. Wählen Sie eine Aktion beim Starten oder Öffnen eines Objekts aus

    - **Blockieren und dem Ereignisprotokoll hinzufügen**. Das Programm blockiert die Ausführung von Objekten oder das Öffnen von Dokumenten, die den Kriterien der Regeln zur Ausführungsprävention entsprechen, und protokolliert im Ereignisprotokoll ein Ereignis zu Versuchen, Objekte zu starten oder Dokumente zu öffnen.

    - **Dem Ereignisprotokoll hinzufügen**. Das Programm protokolliert ein Ereignis zu Versuchen, ausführbare Objekte zu starten oder Dokumente zu öffnen, die den Kriterien der Regeln zur Ausführungsprävention entsprechen, blockiert ihre Ausführung bzw. ihr Öffnen jedoch nicht tatsächlich.

8. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie die Ausführungsprävention für Objekte in den Eigenschaften des verwalteten Geräts

1. Wechseln Sie in der Web Console zu **Asset-Verwaltung** → **Assets (Geräte)**.

2. Klicken Sie auf den Link mit dem Namen des gewünschten Geräts.

3. Dadurch wird das Fenster mit den Eigenschaften des ausgewählten Geräts geöffnet. Wechseln Sie in diesem Fenster zur Registerkarte **Programme** und klicken Sie auf den Link <**Kaspersky Endpoint Security**-Programmname>.

    1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

    2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

       Das Eigenschaftenfenster der Richtlinie wird geöffnet.

    3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

    4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response**.

    5. Gehen Sie zur Registerkarte **Ausführungsprävention**.

    6. Stellen Sie den Umschalter auf **Ausführungsprävention AKTIVIERT**.

    7. Wählen Sie eine Aktion beim Starten oder Öffnen eines Objekts aus

        - **Blockieren und dem Ereignisprotokoll hinzufügen**. Das Programm blockiert die Ausführung von Objekten oder das Öffnen von Dokumenten, die den Kriterien der Regeln zur Ausführungsprävention entsprechen, und protokolliert im Ereignisprotokoll ein Ereignis zu Versuchen, Objekte zu starten oder Dokumente zu öffnen.

        - **Dem Ereignisprotokoll hinzufügen**. Das Programm protokolliert ein Ereignis zu Versuchen, ausführbare Objekte zu starten oder Dokumente zu öffnen, die den Kriterien der Regeln zur Ausführungsprävention entsprechen, blockiert ihre Ausführung bzw. ihr Öffnen jedoch nicht tatsächlich.

    8. Speichern Sie die vorgenommenen Änderungen.

4. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

5. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response**.

6. Wechseln Sie zum Unterabschnitt **Ausführungsprävention**.

7. Stellen Sie den Umschalter auf **Ausführungsprävention AKTIVIERT**.

8. Wählen Sie den Modus der Ausführungsprävention für Objekte aus:

   - **Blockieren**. In diesem Modus blockiert die Anwendung die Ausführung von Objekten oder das Öffnen von Dokumenten, die den Kriterien von Regeln zur Ausführungsprävention entsprechen. Außerdem wird im Ereignisprotokoll über Versuche, ausführbare Objekte zu starten oder Dokumente zu öffnen, ein Ereignis aufgezeichnet.

   - **Informieren**. In diesem Modus protokolliert die Anwendung im Ereignisprotokoll ein Ereignis über Versuche, ausführbare Objekte zu starten oder Dokumente zu öffnen, die den Kriterien von Regeln zur Ausführungsprävention entsprechen, blockiert die Ausführung oder das Öffnen jedoch nicht. Standardmäßig ist dieser Modus ausgewählt.

9. Speichern Sie die vorgenommenen Änderungen.

Das Aktivieren und Deaktivieren der Ausführungsprävention von Objekten ist in den Geräteeigenschaften nicht verfügbar, wenn das Gerät durch eine Richtlinie verwaltet wird ist.

So fügen Sie eine Regel zur Ausführungsprävention für Objekte der Komponente EDR Optimum in der Web Console hinzu

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Aktivieren Sie bei Bedarf das Kontrollkästchen **Groß-/Kleinschreibung beim Pfad berücksichtigen**.

5. Klicken Sie in den Eigenschaften der Richtlinie oder des verwalteten Geräts auf die Schaltfläche **Hinzufügen** in der Symbolleiste oberhalb der Liste der Regeln zur Ausführungsprävention für Objekte.

6. Geben Sie im folgenden Fenster den Namen der Regel zur Ausführungsprävention ein.

7. Geben Sie den Status der Regel zur Ausführungsprävention an, indem Sie den Umschalter auf die entsprechende Position setzen.

8. Wählen Sie in der Dropdown-Liste **Typ** den Typ des Objekts aus, das Sie blockieren möchten:

   - **Ausführbare Datei**.

   - **Skript**.

   - **Datei von Office-Anwendung**.

   Wenn Sie den falschen Objekttyp auswählen, wird die Datei oder das Skript nicht blockiert.

9. Um ein Objekt hinzuzufügen, geben Sie im entsprechenden Feld den Pfad zum Objekt und/oder die Prüfsumme des Objekts (SHA256- oder MD5-Hash der Datei) an.

10. Speichern Sie die vorgenommenen Änderungen.

    Die erstellte Regel wird zur Liste der Regeln im Parameterblock **Ausführungsprävention von Objekten** hinzugefügt.

Kaspersky Endpoint Security kontrolliert die Ausführung ausführbarer Dateien und Skripte sowie das Öffnen von Dateien von Office-Anwendungen auf dem Gerät. Die Ausführungsprävention für Objekte unterstützt eine bestimmte Auswahl von Erweiterungen für Office-Programme und eine bestimmte Auswahl von Skript-Interpretern. Durch das Verbot, Objekte zu starten, kann die Ausbreitung einer Bedrohung gestoppt werden.

Die Ausführungsprävention für Objekte steht in Kaspersky Endpoint Security zur Verfügung, wenn eine der folgenden Bedingungen erfüllt ist:

- Die Integration mit der Lösung Kaspersky Endpoint Detection and Response Optimum ist aktiviert, und die Komponente EDR Optimum ist aktiviert.
- Die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit der Komponente Kaspersky Endpoint Detection and Response (KATA) ist aktiviert, und die Komponente EDR Expert (on-premise) ist aktiviert.
- Die Integration mit Kaspersky Endpoint Detection and Response Expert (cloud) ist aktiviert, und die Komponente EDR Expert (cloud) ist aktiviert.

Wenn der Blockiermodus des Interceptors für Dateioperationen nicht aktiviert ist, arbeitet die Ausführungsprävention für Objekte unabhängig vom festgelegten Betriebsmodus im Benachrichtigungsmodus.

Standardmäßig ist die Ausführungsprävention für Objekte deaktiviert. Das Aktivieren der Ausführungsprävention für Objekte kann sich auf die Startgeschwindigkeit einer Anwendung im Betriebssystem auswirken.

Damit die Ausführungsprävention von Objekten funktioniert, müssen Sie die Anwendung der Regel zur Ausführungsprävention von Objekten aktivieren.

Einschränkungen und Besonderheiten der Ausführungsprävention für Objekte

Einschränkungen der Ausführungsprävention für Objekte

Für die Ausführungsprävention für Objekte, gelten die folgenden Einschränkungen:

- Objekte, die in Regeln der Ausführungsprävention angegeben sind, werden erst nach dem Start von Kaspersky Endpoint Security blockiert.
- Kaspersky Endpoint Security blockiert keine Dateien, die während der Erstellung oder Änderung der Regel zur Ausführungsprävention geöffnet sind.
- Das Kaspersky Endpoint Security blockiert nicht die Arbeit mit Objekten, die vor der Erstellung oder Änderung einer Regel der Ausführungsprävention gestartet wurden und den neu definierten Regeln entsprechen.
- Bestimmte Dateien können für den Betrieb des Betriebssystems und der Anwendung von kritischer Bedeutung sein. Die Ausführungsprävention für solche Dateien kann die Funktionen des Betriebssystems stören.

Es wird nicht empfohlen, mehr als 50.000 Regeln für die Ausführungsprävention zu erstellen. Andernfalls kann es zu Systeminstabilitäten kommen.

Besonderheiten der Ausführungsprävention für Objekte bei der Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) und Kaspersky Endpoint Detection and Response (KATA)

Bei der Integration des Programms Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder Kaspersky Endpoint Detection and Response (KATA) verwendet die Anwendung die *Regeln zur Ausführungsprävention für Objekte der Komponente EDR Expert (on-premise)*. Diese Regeln erhält die Anwendung von Kaspersky Endpoint Detection and Response Expert (on-premise) oder von Kaspersky Endpoint Detection and Response (KATA).

Bei der Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA) können Sie:

- Die Anwendung der Regeln zur Ausführungsprävention für Objekte der Komponente EDR Expert (on-premises) in der Web Console oder in der Verwaltungskonsole aktivieren oder deaktivieren.

  Wenn Regeln zur Ausführungsprävention ausgelöst werden, sendet Kaspersky Endpoint Security einen Bericht an Endpoint Detection and Response Expert (on-premise) oder an die Kaspersky Anti Targeted Attack Platform. Weitere Informationen dazu finden Sie in der Hilfe der jeweiligen Lösung.

- Die Liste der Regeln zur Ausführungsprävention für Objekte der Komponente EDR Expert (on-premise) über die Befehlszeile anzeigen.

Besonderheiten der Ausführungsprävention für Objekte bei der Integration mit Kaspersky Endpoint Detection and Response Optimum

Bei einer Integration der Anwendung "Kaspersky Endpoint Security" mit der Lösung "Kaspersky Endpoint Detection and Response Optimum" verwendet die Anwendung die *Regeln zur Ausführungsprävention von Objekten der Komponente "EDR Optimum"*. Diese Regeln erstellen Sie manuell in der Web Console. Sie können Regeln für die Ausführungsprävention auch automatisch im Fenster mit den Alarm-Details erstellen.

Bei der Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie Folgendes tun:

- Die Anwendung der Regeln zur Ausführungsprävention für Objekte der Komponente EDR Optimum in der Web Console aktivieren oder deaktivieren.

- Regeln zur Ausführungsprävention für Objekte der Komponente EDR Optimum in der Web Console erstellen und konfigurieren.

  Sie können auch automatisch eine Regel für die Ausführungsprävention für ein Objekt erstellen, indem Sie im Fenster mit den Alarm-Details die Ausführung einer Datei verhindern. Die Regel der Ausführungsprävention wird der Richtlinie jener Administrationsgruppe hinzugefügt, zu der das Gerät gehört.

  > Sie können die Ausführung von Dateien im Fenster mit den Alarmdetails nur dann blockieren, wenn das Gerät von einer Richtlinie abgedeckt wird.

- Die Liste mit den Regeln der Ausführungsprävention von Objekten der Komponente "EDR Optimum" in der Befehlszeile anzeigen.

Bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum kann die Ausführungsprävention für Objekte in einem von zwei Modi erfolgen:

- **Blockieren**. In diesem Modus blockiert die Anwendung die Ausführung von Objekten oder das Öffnen von Dokumenten, die den Kriterien von Regeln zur Ausführungsprävention entsprechen. Außerdem wird im Protokoll über Versuche, ausführbare Objekte zu starten oder Dokumente zu öffnen, ein Ereignis aufgezeichnet.

  Kaspersky Endpoint Security blockiert die Ausführung von Skripten, die durch die Ausführungsprävention verboten sind, auch wenn sie von einem erlaubten Skript importiert wurden.

- **Informieren**. In diesem Modus protokolliert die Anwendung Ereignisse über Versuche, ausführbare Objekte zu starten oder Dokumente zu öffnen, die den Kriterien von Regeln zur Ausführungsprävention entsprechen, blockiert die Ausführung oder das Öffnen jedoch nicht. Standardmäßig ist dieser Modus ausgewählt.

Quarantäne verwenden

Die *Quarantäne* ist ein spezieller Speicher auf dem Gerät, in dem Dateien abgelegt werden, die möglicherweise mit Viren infiziert sind oder die zum Zeitpunkt der Erkennung nicht desinfiziert werden können. Mithilfe der Quarantäne können Sie eine Datei zur weiteren Überprüfung isolieren. Dateien in der Quarantäne werden in verschlüsselter Form gespeichert und stellen keine Gefahr für das Gerät dar. Im Gegensatz zur Quarantäne dient der Backup-Speicher dazu, Backup-Kopien von Dateien zu speichern, in denen Schadcode gefunden wurde und die während des Desinfektionsprozesses gelöscht oder geändert wurden.

Die Anwendung verwendet nur bei einer Integration mit Detection and Response-Lösungen die Quarantäne, um empfohlene Maßnahmen zur Reaktion auf eine Bedrohung durchzuführen. Wenn Sie die Anwendung mit Kaspersky Endpoint Detection and Response Optimum oder Kaspersky Managed Detection and Response integrieren, können Sie Dateien, die Sie als gefährlich für Ihr Gerät einstufen, auch manuell in die Quarantäne verschieben.

Für Backup-Kopien von Dateien, die in die Quarantäne verschoben wurden, wird standardmäßig das Verzeichnis "/var/opt/kaspersky/kesl/common/objects-backup/" verwendet. In diesem Verzeichnis werden auch Objekte des Backup-Speichers gespeichert. Sie können das Speicherverzeichnis für die Objekte des Backup-Speichers und der Quarantäne über die Befehlszeile ändern.

Dateien in der Quarantäne können persönliche Daten enthalten. Für den Zugriff auf Dateien, die in die Quarantäne verschoben wurden, sind Root-Rechte erforderlich.

Sie können die Quarantäne-Einstellungen auf einem Gerät mithilfe einer Richtlinie in der Web Console oder in der Verwaltungskonsole oder über die Befehlszeile konfigurieren. Sie können die folgenden Einstellungen der Quarantäne konfigurieren:

- Füllstand der Quarantäne in Prozent, bei dessen Erreichen eine Ereignis über mangelnden Quarantäne-Speicher generiert werden soll. Standardmäßig wird ein Ereignis generiert, wenn die Quarantäne zu 90% gefüllt ist.

- Maximale Größe der Quarantäne in Megabyte. Wenn die maximale Größe der Quarantäne erreicht wird, löscht die Anwendung automatisch die ältesten Dateien aus der Quarantäne. Die maximale Größe der Quarantäne beträgt standardmäßig 200 MB, wenn das Programm im Standard-Modus oder EDR Agent-Modus verwendet wird, und 100 MB, wenn das Programm im Light Agent-Modus verwendet wird.

- Pfad zum Verzeichnis, in dem die Objekte des Backup-Speichers und der Quarantäne gespeichert werden (dieser Parameter kann nur über die Befehlszeile geändert werden).

So verwalten Sie die Quarantäne-Einstellungen in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Berichte und Speicher**.
5. Konfigurieren Sie im Abschnitt **Quarantäne** die folgenden Einstellungen:

   - **Maximale Größe der Quarantäne**. Beschränkung der Quarantäne auf die angegebene Größe in Megabyte. Dieses Kontrollkästchen ist standardmäßig aktiviert.
   - **Maximale Quarantäne-Größe (MB)**. Wenn die Einstellung **Maximale Größe der Quarantäne** aktiviert ist, können Sie die maximale Größe der Quarantäne in Megabyte angeben (standardmäßig 200 MB). Die Größe der Quarantäne darf 999.999 MB nicht überschreiten.
   - **Benachrichtigen, wenn Quarantäne voll ist**. Benachrichtigungen, wenn die Quarantäne diesen Füllstand in Prozent erreicht. Dieses Kontrollkästchen ist standardmäßig aktiviert.

     Sie können den Prozentsatz angeben, ab dem eine Benachrichtigung gesendet wird (standardmäßig 90 %).
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Dateien in die Quarantäne verschieben

Bestimmte Dateien können für den Betrieb des Betriebssystems und der Anwendung von kritischer Bedeutung sein. Wenn solche Dateien in die Quarantäne verschoben werden, kann der Systembetrieb gestört werden.

Das Verschieben einer Datei in die Quarantäne ist nur möglich, wenn eine der folgenden Bedingungen erfüllt ist:

- Die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Optimum ist aktiviert, und die Komponente EDR Optimum ist aktiviert.
- Die Integration des Programms Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit der Komponente Kaspersky Endpoint Detection and Response (KATA) ist aktiviert, und die Komponente EDR Expert (on-premise) ist aktiviert.
- Die Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response ist aktiviert, und die Komponente MDR ist aktiviert.

Für das Verzeichnis zum Speichern der Quarantäneobjekte sollte Schreibzugriff verfügbar sein.

Bei der Integration mit Kaspersky Endpoint Detection and Response (on-premise) oder Kaspersky Endpoint Detection and Response (KATA) können Dateien auf eine der folgenden Arten in die Quarantäne verschoben werden:

- Als Ausführungsergebnis einer Aufgabe, die in der jeweiligen Managed Detection and Response-Lösung konfiguriert ist. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premise) oder in der Hilfe zu Kaspersky Anti Targeted Attack Platform.
- Als Ergebnis der Ausführung der Aufgabe zur IOC-Untersuchung im Prozessspeicher.

Bei der Integration mit Kaspersky Managed Detection and Response werden Dateien auf eine der folgenden Arten unter Quarantäne gestellt:

- Als Ausführungsergebnis einer Aufgabe, die auf der Seite von Kaspersky Managed Detection and Response konfiguriert ist.
- Als Ausführungsergebnis eines Befehls zur Verwaltung der Quarantäne auf dem Gerät.

Weitere Informationen zum Arbeiten mit Quarantäne bei einer Integration mit Kaspersky Managed Detection and Response finden Sie in der Hilfe zu Kaspersky Managed Detection and Response.

Bei der Integration mit Kaspersky Endpoint Detection and Response Optimum werden Dateien auf eine der folgenden Arten unter Quarantäne gestellt:

- Automatisch als Ergebnis der Erkennung von Kompromittierungsindikatoren.
- Als Ergebnis der Ausführung der Aufgabe Datei in die Quarantäne verschieben, die Sie in der *Web Console* erstellen können.
- Als Ausführungsergebnis eines Befehls zur Verwaltung der Quarantäne auf dem Gerät.
- Durch Befolgen der Empfehlung in den Alarm-Details.

Weitere Informationen zum Arbeiten mit Quarantäne bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum.

Mit Dateien in der Quarantäne arbeiten

Sie können mit Dateien, die in die Quarantäne verschoben wurden, arbeiten:

- In Kaspersky Security Center in der allgemeinen Liste von Dateien, die durch Kaspersky-Anwendungen in die Quarantäne verschoben wurden.

  Um Aktionen mit Dateien in der Quarantäne in Kaspersky Security Center durchzuführen, müssen Sie die Übertragung von Daten über Quarantäne-Dateien an den Administrationsserver aktivieren.

- Lokal auf dem Gerät über die Befehlszeile.

Sie sowohl Informationen zu Dateien anzeigen, die sich in der Quarantäne befinden, als auch diese Dateien aus der Quarantäne löschen und wiederherstellen.

Das Wiederherstellen, Löschen und Abrufen einer Datei aus der Quarantäne ist unabhängig davon möglich, ob die Integration mit Detection and Response-Lösungen aktiviert ist und ob das Gerät durch eine Richtlinie abgedeckt ist.

Eine Liste der von Kaspersky-Lab-Anwendungen auf Client-Geräten unter Quarantäne gestellten Dateien wird in Kaspersky Security Center erstellt und ist in der Verwaltungskonsole (**Erweitert** → **Speicher** → **Quarantäne**) und in der Web Console (**Vorgänge** → **Quarantäne** → **Quarantäne**) verfügbar. Kaspersky Security Center kopiert keine Dateien aus dem Quarantäne-Speicher auf den Administrationsserver. Stattdessen werden alle Dateien im Quarantäne-Speicher auf geschützten Geräten abgelegt. Ausführliche Informationen zur Verwaltung von Dateien in Quarantäne in Kaspersky Security Center finden Sie in der Hilfe zu Kaspersky Security Center.

Die in die Quarantäne verschobenen Dateien werden gemäß den angegebenen Parametern an ihren ursprünglichen Speicherorten wiederhergestellt. Das Mandanten-Tag (nur auf Geräten mit dem Betriebssystem Astra Linux) und die Attribute (einschließlich "immutable" und "append-only") der ursprünglichen Datei werden bei der Wiederherstellung beibehalten. Eine Datei mit den Attributen "immutable" und "append-only" kann nur an einem angegebenen Ort, an dem die Originaldatei nicht existiert, oder unter einem anderen Namen am ursprünglichen Ort wiederhergestellt werden. Das Wiederherstellen einer Datei aus der Quarantäne in ein anderes Verzeichnis oder an ihren ursprünglichen Speicherort unter einem anderen Namen erfordert Root-Berechtigungen.

Sobald die Wiederherstellung abgeschlossen ist, löscht die Anwendung die Kopie der wiederhergestellten Datei aus der Quarantäne.

Das Wiederherstellen einer Datei aus der Quarantäne schlägt in den folgenden Fällen mit einem Fehler fehl:

- Die wiederherzustellende Datei konnte im Speicher der Quarantäne nicht gefunden werden.
- Der eingegebene Name der wiederherzustellenden Datei ist falsch oder besitzt eine fehlerhafte Groß- und Kleinschreibung.
- Die angegebene ID der Datei ist falsch.
- Entweder wurde das Zielverzeichnis gelöscht, verschoben oder umbenannt, oder Sie haben keine Zugriffsberechtigung auf den Ordner.

  In diesem Fall verschiebt die Anwendung die Datei in das Verzeichnis /var/opt/kaspersky/kesl/common/restored/. Sie können die Datei manuell aus diesem Verzeichnis in das gewünschte Verzeichnis verschieben.
- Im angegebenen Pfad ist bereits eine Datei mit demselben Namen vorhanden.
- Zu wenig Speicherplatz auf dem Gerät.
- Nur auf Geräten mit Astra Linux-Betriebssystemen gilt: Das Mandanten-Tag der Datei ist höher als das Mandanten-Tag des Verzeichnisses, in dem die Datei wiederhergestellt wird.
- Nur auf Geräten mit Astra Linux-Betriebssystemen gilt: Das Mandanten-Tag der Datei ist niedriger als das Mandanten-Tag des Verzeichnisses, in dem die Datei wiederhergestellt wird, und für das Verzeichnis wurde das Flag "ccnr" nicht angegeben.

Das Löschen einer Datei aus der Quarantäne schlägt in den folgenden Fällen mit einem Fehler fehl:

- Die zu löschende Datei konnte im Speicher der Quarantäne nicht gefunden werden.
- Der eingegebene Name der zu löschenden Datei ist falsch oder besitzt eine fehlerhafte Groß- und Kleinschreibung.
- Die angegebene ID der Datei ist falsch.

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 Security 12.5 für Linux ist mit Kaspersky Endpoint Detection and Response Optimum Version 3.1 kompatibel.

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*).

Verwenden Sie für die zentrale Verwaltung des Programms Kaspersky Endpoint Security mit der Komponente EDR Optimum Kaspersky Security Center Windows 15.1 oder Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2.

Die Komponente ist für Geräte mit Elbrus-CPU nicht verfügbar.

Funktionsweise von Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum überwacht und analysiert die Entwicklung von Bedrohungen und stellt einem Security Officer oder Administrator Informationen über einen potenziellen Angriff zur Verfügung, damit diese rechtzeitig Maßnahmen zur Reaktion auf Bedrohungen ergreifen können.

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 Security Center neben Überwachungsdaten zu Prozessen, offenen Netzwerkverbindungen und geänderten Dateien auch Daten zu den von der Anwendung erkannten Bedrohungen und zu den Verarbeitungsergebnissen dieser Bedrohungen.
- Ausführen von Reaktionsmaßnahmen, welche darauf abzielen, auf Grundlage von Befehlen, die von Kaspersky Security Center empfangen wurden, die Schutzfunktionen zu gewährleisten.

Konfigurieren der Integration mit Kaspersky Endpoint Detection and Response Optimum

Voraussetzungen

Vor dem Konfigurieren der Integration mit Kaspersky Endpoint Detection and Response Optimum:

- Fügen Sie dem Programm den EDR Optimum-Lizenzschlüssel hinzu, wenn Sie eine separate Lizenz zur Nutzung dieser Funktionalität erworben haben.

  Wenn Sie Kaspersky Endpoint Security mit einer Lizenz, die Kaspersky Endpoint Detection and Response Optimum umfasst, verwenden, ist keine Aktion erforderlich.

  > Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, wird der Lizenzschlüssel zur SVM hinzugefügt.

- Stellen Sie sicher, dass Folgendes aktiviert ist und funktioniert:

  - Kaspersky Security Network im Standardmodus oder im erweiterten Modus:

    > Für eine optimale Ausführung von Kaspersky Endpoint Detection and Response Optimum wird es empfohlen, Kaspersky Security Network im erweiterten Modus zu verwenden.

  - Die folgenden Komponenten des Programms Kaspersky Endpoint Security:

    - Schutz vor bedrohlichen Dateien.
    - Verhaltensanalyse.

  Um sicherzustellen, dass die Telemetriedaten vollständig sind, und um in Kaspersky Security Center eine Bedrohungsentwicklungskette zu erstellen, müssen Sie zusätzlich Schutz vor Web-Bedrohungen aktivieren.

  Sie können auch die Ausführungsprävention für Objekte aktivieren.

Grundlegende Konfigurationsschritte

1. **Installieren Sie das Verwaltungs-Plug-in für Kaspersky Endpoint Detection and Response Optimum**

   Das Verwaltungs-Plug-in für Kaspersky Endpoint Detection and Response Optimum ist ein vereinheitlichtes Plug-in für die Arbeit mit Agenten unter Windows-, Mac- und Linux-Betriebssystemen und wird zum Anzeigen von Alarmdetails benötigt. Eine Beschreibung des Installationsverfahrens finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum.

   Wenn in Ihrer Infrastruktur die Kaspersky Security Center Cloud Console für die Verwaltung von Kaspersky Endpoint Detection and Response Optimum verwendet wird, ist das Plug-in standardmäßig installiert.

2. **Konfigurieren Sie die Einstellungen für die Integration mit Kaspersky Endpoint Detection and Response Optimum**

Diese können Sie wie folgt konfigurieren:

- Mithilfe der Web Console (Kaspersky Security Center Console und/oder OSMP-Konsole).
- Über die Befehlszeile

> Die Verwaltung von EDR Optimum über die Verwaltungskonsole von Kaspersky Security Center wird nicht unterstützt.

3. **Aktivieren Sie die Datenübertragung zum Administrationsserver**

   Um alle Funktionen von Kaspersky Endpoint Detection and Response Optimum zu verwenden, müssen Sie die folgenden Einstellungen konfigurieren:

   - Aktivieren Sie das Senden von Informationen über Dateien im Backup und in der Quarantäne an den Speicher von Kaspersky Security Center. Dazu müssen Sie in den Richtlinieneigenschaften die folgenden Kontrollkästchen aktivieren:
     - **Dateien im Backup**
     - **Dateien in der Quarantäne**
   - Aktivieren Sie die Anzeige der Alarmliste. Dazu können Sie im Hauptfenster der Kaspersky Security Center Web Console unter **Einstellungen** → **Einstellungen der Benutzeroberfläche** den Umschalter **EDR-Alarme anzeigen** aktivieren.

     > In der Web Console bis Version 15.1 ist die Option **EDR-Alarme anzeigen** nicht verfügbar. Sie können aus dem Bericht über Bedrohungen in der Kaspersky Security Center-Konsole zu EDR-Alarmen wechseln.

   - Aktivieren Sie die Übertragung von Informationen über Ereignisse von Drittanbieter-Programmen auf verwalteten Geräten. Führen Sie dazu auf dem verwalteten Gerät den folgenden Befehl aus:

     ```
     kesl-control --set-app-settings SystemEventsTransmission=Yes
     ```

     > Die Aktivierung dieser Einstellung kann die Auslastung des Betriebssystems erheblich erhöhen.

4. **Stellen Sie sicher, dass die Verbindung zu Kaspersky Endpoint Detection and Response Optimum erfolgreich hergestellt wurde**

   Überprüfen Sie den Status von Kaspersky Endpoint Detection and Response Optimum auf eine beliebige geeignete Weise.

Die Integration mit Kaspersky Endpoint Detection and Response Optimum ist konfiguriert. Wenn eine Bedrohung erkannt wird, wird ein Alarm generiert. Im Fenster „Alarm-Details“ können Sie Informationen zur Bedrohung anzeigen und Reaktionsaktionen ausführen.

So aktivieren Sie die Integration mit EDR Optimum

In der Web Console können Sie die Komponente „EDR Optimum“ aktivieren oder deaktivieren und in den Richtlinieneigenschaften die Integration mit Kaspersky Endpoint Detection and Response Optimum konfigurieren.

So aktivieren Sie die Integration mit Kaspersky Endpoint Detection and Response Optimum in der Web Console

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response**.
5. Aktivieren Sie den Umschalter **Endpoint Detection and Response AKTIVIERT**.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren Sie die Integration mit Kaspersky Endpoint Detection and Response Optimum über die Befehlszeile

Führen Sie den folgenden Befehl aus, um die Komponente EDR Optimum zu aktivieren:

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

1. Wählen Sie im Hauptfenster der Web Console den Abschnitt **Asset-Management** → **Assets (Geräte)** aus.
2. Klicken Sie auf den Link mit dem Namen des gewünschten Geräts.
3. Daraufhin wird das Eigenschaftenfenster des ausgewählten Geräts geöffnet; wechseln Sie in diesem Fenster zur Registerkarte **Programme** und klicken Sie auf den Link <Name des Programms „Kaspersky Endpoint Security“>.
4. Wechseln Sie zur Registerkarte **Programmeinstellungen**, klicken Sie auf den Abschnitt **Detection and Response** und klicken Sie anschließend auf den Link **Endpoint Detection and Response Optimum**.
5. Daraufhin wird ein Fenster geöffnet; stellen Sie in diesem Fenster den Umschalter auf **Endpoint Detection and Response Optimum aktiviert** ein, um die Integration zu aktivieren.
6. Verwalten Sie bei Bedarf die folgenden Einstellungen:

   - Dauer der Geräteblockierung im Rahmen der automatischen Netzwerkisolation.

     Klicken Sie auf den Link **Geräteentsperrung konfigurieren** und geben Sie die Blockierungsdauer an.
   - Ausnahmen für die automatische Netzwerkisolation
7. Speichern Sie die vorgenommenen Änderungen.

Das verwaltete Gerät ist für die Integration mit Kaspersky Endpoint Detection and Response Optimum konfiguriert.

So überprüfen Sie, ob die EDR Optimum-Integration ordnungsgemäß funktioniert

Lesen Sie die Informationen zu den möglichen Integrationsstatus und dazu, wann sie angezeigt werden können.

Sie können die Komponente EDR Optimum auf folgende Arten testen:

- Über die Befehlszeile mit folgendem Befehl:

  ```
  kesl-control --app-info
  ```

  Die EDR Optimum-Integration wird mit dem Status **Wird ausgeführt** angezeigt.

- In der Web Console:

  - Mithilfe des *Berichts über den Status der Programmkomponenten*. Weitere Informationen zum Umgang mit Berichten finden Sie in der Hilfe zu Kaspersky Security Center.

  - Wechseln Sie zum Abschnitt **Asset-Management** → **Assets** → Link <Gerätename> → Registerkarte **Programme** → Link <Name des Programms Kaspersky Endpoint Security> → Registerkarte **Allgemein** → **Komponenten**.

    Die Komponente Endpoint Detection and Response Optimum wird mit dem Status **Wird ausgeführt** angezeigt.

Cloud Sandbox

Mit der Technologie *Cloud Sandbox* können Sie komplexe Bedrohungen auf einem Computer erkennen. Kaspersky Endpoint Security leitet erkannte Dateien automatisch zur Analyse an „Cloud Sandbox“ weiter. Cloud Sandbox führt diese Dateien in einer isolierten Umgebung aus, um bösartige Aktivitäten zu erkennen und Entscheidungen über die Reputation dieser Dateien zu treffen. Daten über diese Dateien werden an Kaspersky Security Network gesendet. Wenn „Cloud Sandbox“ eine schädliche Datei gefunden hat, führt Kaspersky Endpoint Security die passende Aktion aus, um diese Bedrohung auf allen Computern, auf denen die Bedrohung vorliegt, zu beseitigen.

Damit „Cloud Sandbox“ funktioniert, müssen Sie die Verwendung von Kaspersky Security Network aktivieren.

Wenn Sie Kaspersky Private Security Network verwenden, ist die Cloud-Sandbox-Technologie nicht verfügbar.

Die Cloud-Sandbox-Technologie ist immer aktiviert und für alle Benutzer von Kaspersky Security Network verfügbar, unabhängig vom Typ der verwendeten Lizenz. Wenn Sie die Lösung Endpoint Detection and Response Optimum bereits bereitgestellt haben, können Sie einen separaten Indikator für durch Cloud Sandbox erkannte Bedrohungen aktivieren. Diesen Indikator können Sie verwenden, um bei der Analyse erkannter Bedrohungen Statistiken zu erstellen. Kaspersky Endpoint Security zeigt die Technologie zur Erkennung von Bedrohungen durch Cloud Sandbox im *Bericht über Bedrohungen* in der Kaspersky Security Center-Konsole an.

So aktivieren Sie den Zähler für Cloud Sandbox in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response**.
5. Wählen Sie die Registerkarte **Cloud Sandbox** aus.
6. Aktivieren Sie den Umschalter **Cloud Sandbox AKTIVIERT**.
7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Endpoint Detection and Response Expert (On-Premises)

Kaspersky Endpoint Detection and Response Expert (on-premise) ist eine Cybersicherheitslösung für Unternehmen, mit der Sie sich vor den meisten Cybersicherheitsrisiken schützen und die wichtigsten Szenarien der Ausbreitung von Bedrohungen abdecken können. Die Komponenten von Kaspersky Endpoint Detection and Response Expert (on-premise) werden auf der Open Single Management Platform (OSMP) bereitgestellt. Weitere Informationen zur Lösung und zur Plattform finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premise).

Die Integration mit der Lösung Kaspersky Endpoint Detection and Response Expert (on-premise) wird durch die Komponente Endpoint Detection and Response Expert (on-premise) von Kaspersky Endpoint Security bereitgestellt (im Folgenden auch als *EDR Expert (on-premise)* bezeichnet).

Die Komponente ist für Geräte mit Elbrus-CPU nicht verfügbar.

Funktionsweise von Endpoint Detection and Response Expert (on-premise)

1. **Geräte mit Kaspersky Endpoint Security stellen sichere Verbindungen zum OSMP-Server für Aktionen zur Reaktion auf Bedrohungen und zum OSMP-Server für die Erfassung von Telemetriedaten her**
2. **Kaspersky Endpoint Security sendet Daten an den Server für die Erfassung von Telemetriedaten auf der OSMP-Plattform**

   Die folgenden Informationen werden übermittelt:

   - Informationen zu Ereignissen auf dem Gerät
   - Informationen zu den vom Programm erkannten Bedrohungen
   - Informationen zu den Ergebnissen der Verarbeitung dieser Bedrohungen
   - Überwachungsdaten zu Prozessen, offenen Netzwerkverbindungen und geänderten Dateien

3. **Kaspersky Endpoint Security führt Aktionen zur Reaktion auf Bedrohungen aus**

   Aktionen zur Reaktion werden auf Befehl des Servers für Aktionen zur Reaktion auf Bedrohungen auf der OSMP-Plattform ausgeführt.

Integration in Kaspersky Endpoint Detection and Response Expert (on-premise) konfigurieren

Voraussetzungen

Vor der Konfiguration der Integration in Kaspersky Endpoint Detection and Response Expert (on-premise):

- Lassen Sie Verbindungen über die Ports 443 und 8443 zu.
- Aktivieren Sie die Komponente Verhaltensanalyse, um die erforderlichen Telemetriedaten zu übertragen.

  Wenn Sie Informationen über erkannte Bedrohungen von anderen Schutzkomponenten erhalten möchten, aktivieren Sie diese Komponenten:

  - Schutz vor bedrohlichen Dateien.
  - Schutz vor Netzwerkbedrohungen.
  - Schutz vor Web-Bedrohungen.
  - Schutz vor Verschlüsselung.
  - Programmkontrolle.
  - Gerätekontrolle.
  - Überwachung der Systemintegrität.

  > Wenn Sie in der Komponente "Verhaltensanalyse" den eBPF-Mechanismus zum Abrufen von Telemetriedaten des Systems verwenden (verfügbar auf 64-Bit-Betriebssystemen mit Kernelversion 4.18 und höher mit eBPF-Unterstützung), sind die Telemetriedaten vollständiger.

- Fügen Sie dem Programm den Lizenzschlüssel für EDR Expert (on-premise) hinzu, wenn Sie eine separate Lizenz zur Nutzung dieser Funktionalität erworben haben.

  Wenn Sie Kaspersky Endpoint Security mit einer Lizenz, die Kaspersky Endpoint Detection and Response Expert (on-premise) umfasst, verwenden, ist keine Aktion erforderlich.

  Wenn das Programm im Light Agent-Modus verwendet wird, wird der Lizenzschlüssel für EDR Expert (on-premise) zur SVM hinzugefügt.

- Außerdem müssen Sie auf der OSMP-Plattform einen Kollektor, einen Korrelator und einen Speicher konfigurieren.

Grundlegende Konfigurationsschritte

1. **Abrufen und Verarbeiten der von den OSMP-Servern ausgestellten Zertifikate**

Bei der Integration in Kaspersky Endpoint Detection and Response Expert (on-premise) stellen Geräte, auf denen Kaspersky Endpoint Security ausgeführt wird, verschlüsselte HTTPS-Verbindungen zum OSMP-Server für die Reaktion auf Bedrohungen und zum OSMP-Telemetrieserver her.

Wenn in den allgemeinen Einstellungen von Kaspersky Endpoint Security die Verwendung eines Proxyservers konfiguriert ist, wird dieser für die Verbindung zu OSMP-Servern verwendet.

Die Zertifikate zum Absichern der Verbindungen mit den OSMP-Servern werden vom Administrator der OSMP-Plattform bereitgestellt.

Um Zertifikate zu verarbeiten, führen Sie die Schritte aus, die im Artikel Konvertieren eines PFX-Zertifikats in das PEM-Format beschrieben sind.

Sie können ein Serverzertifikat und/oder ein Client-Zertifikat verwenden. Die Auswahl richtet sich nach der Sicherheitsrichtlinie Ihrer Organisation.

2. **Integrationseinstellungen für Kaspersky Endpoint Detection and Response Expert (on-premise) konfigurieren**

   Diese können Sie wie folgt konfigurieren:

   - Mithilfe der Web Console (Kaspersky Security Center Console und/oder OSMP-Konsole).
   - Über die Befehlszeile

   Wenn Sie die Ausführungsprävention für Objekte verwenden möchten, können Sie die Regeln für die Ausführungsprävention für Objekte der Komponente EDR Expert (on-premise) aktivieren.

3. **Überprüfen, ob die Verbindung mit der Plattform Endpoint Detection and Response Expert (on-premise) erfolgreich hergestellt wurde**

   Überprüfen Sie den Status von EDR Expert (on-premise) auf beliebige geeignete Weise.

4. **Bei Bedarf zusätzliche Einstellungen verwalten**

   - Wenn SELinux in Ihrem Betriebssystem im Enforcing-Modus konfiguriert ist, müssen Sie SELinux zusätzlich konfigurieren, um Reaktionsaktionen auszuführen.
   - Um die Aktion zur Reaktion **Speicherauszug** oder **Prozess-Dump** auszuführen, entsperren Sie ptrace.
   - Machen Sie sich mit den Einschränkungen der Netzwerkisolation vertraut.
   - Aktivieren Sie die Übertragung von Informationen über Ereignisse von Drittanbieter-Programmen auf verwalteten Geräten. Führen Sie dazu auf dem verwalteten Gerät den folgenden Befehl aus:

     ```
     kesl-control --set-app-settings SystemEventsTransmission=Yes
     ```

     Die Aktivierung dieser Einstellung kann die Auslastung des Betriebssystems erheblich erhöhen.

So bereiten Sie ein Referenzabbild für die korrekte Integration mit EDR Expert (on-premises) vor

Vergewissern Sie sich vor der Vorbereitung des Abbilds, dass die Datei `/var/opt/kaspersky/.ids_generated` auf dem Referenzgerät nicht vorhanden ist.

So bereiten Sie ein Referenzimage für die korrekte Integration mit Kaspersky Endpoint Detection and Response Expert (on-premises) vor:

Starten Sie das Referenzgerät oder Kaspersky Endpoint Security nicht neu, während Sie diese Anweisungen befolgen.

1. Führen Sie die folgenden Befehle als root aus:

   ```
   systemctl stop kesl
   systemctl edit kesl
   ```

2. Fügen Sie im Editor zwischen den Zeilen `### Anything between here and the comment below will become the contents of the drop-in file` und `### Edits below this comment will be discarded` eine der folgenden Konfigurationen hinzu:

   - Aktualisieren Sie die SensorID bei jedem Start des Programms auf temporären virtuellen Maschinen

     ```
     [Service]
     ExecStartPre=-/usr/bin/uuid-regen.sh -a
     ```

   - Aktualisieren Sie die SensorID nur einmal auf persistenten virtuellen Maschinen

     ```
     [Service]
     ExecStartPre=-/usr/bin/uuid-regen.sh -b
     ```

3. Speichern Sie Ihre Änderungen und schließen Sie den Editor.

   Die Datei `/etc/systemd/system/kesl.d/override.conf` wird erstellt. Überprüfen Sie den Inhalt, um sicherzustellen, dass er mit der hinzugefügten Konfiguration übereinstimmt.

4. Laden Sie den systemd-Dienst neu, indem Sie den folgenden Befehl ausführen:

   ```
   systemctl daemon-reload
   ```

5. Erstellen Sie die Datei `/usr/bin/uuid-regen.sh` mit folgendem Inhalt:

```
#!/usr/bin/env bash
# ------------------------------------------------------------
#  Kaspersky IDs updater
#  Modes:
#    -a   Always regenerate the IDs (default)
#    -b   Generate them only once – subsequent runs do nothing
#  Exit code: always 0
# ------------------------------------------------------------
set -euo pipefail
# ----- configuration ------------------------------------------------
PCID_FILE="/var/opt/kaspersky/kesl/common/pcid"
INSTALL_ID_FILE="/var/opt/kaspersky/epagent/install_id"
KESL_INI="/var/opt/kaspersky/kesl/common/kesl.ini"
# Marker that shows the script has already been executed in mode b
MARKER="/var/opt/kaspersky/.ids_generated"
# ----- default mode -------------------------------------------------
MODE="a"
# ----- parse command-line arguments ---------------------------------
while getopts ":ab" opt; do
   case $opt in
       a) MODE="a" ;;
       b) MODE="b" ;;
       \?) echo "Invalid option: -$OPTARG" >&2; exit 0 ;;
   esac
done
shift $((OPTIND-1))
# ----- helper: generate a new UUID and write to a file --------------
write_uuid() {
   local target=$1
   /usr/bin/uuidgen > "$target"
}
# ----- helper: replace MachineId in kesl.ini ------------------------
replace_machine_id() {
   local new_id
   new_id=$(/usr/bin/uuidgen)
   /usr/bin/sed -i "s/^MachineId=.*/MachineId=${new_id}/" "$KESL_INI"
}
# ----- main logic ---------------------------------------------------
if [[ "$MODE" == "b" && -f "$MARKER" ]]; then
   # Mode b – already ran once → do nothing
   :
else
   # (re)generate all required values
   write_uuid "$PCID_FILE"
   write_uuid "$INSTALL_ID_FILE"
   replace_machine_id
   # In mode b remember that we have already executed
   if [[ "$MODE" == "b" ]]; then
       /usr/bin/touch "$MARKER"
   fi
fi
exit 0
```

6. Ändern Sie die Berechtigungen der Datei `/usr/bin/uuid-regen.sh` mit folgendem Befehl:

```
chmod 700 /usr/bin/uuid-regen.sh
```

Das Referenzgerät ist jetzt für die Erstellung des Betriebssystemabbilds bereit.

So konfigurieren Sie die Integration von EDR Expert (on-premise)

In der Web Console können Sie die Komponente EDR Expert (on-premise) aktivieren oder deaktivieren und die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Expert (on-premise) in den Eigenschaften der Kaspersky Endpoint Security-Richtlinie konfigurieren.

So konfigurieren Sie die Integration von Kaspersky Endpoint Detection and Response Expert (on-premise) in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response Expert (On-Premises)**.
5. Wählen Sie die Option **Endpoint Detection and Response Expert Version 8.0 oder höher** aus.
6. Fügen Sie Server zur Erfassung von Telemetriedaten und Server für die Reaktion auf Bedrohungen hinzu.

   Klicken Sie hierzu in den Abschnitten **Verbindung mit Servern zur Erfassung von Telemetriedaten** und **Verbindung mit Servern für die Reaktion auf Bedrohungen** auf die Schaltfläche **Hinzufügen**. Geben Sie in dem angezeigten Fenster die Serveradresse (IPv4, IPv6) und den Port für die Serververbindung an.
7. Fügen Sie Zertifikate hinzu, indem Sie in den Abschnitten **Verbindung mit Servern zur Erfassung von Telemetriedaten** und **Verbindung mit Servern für die Reaktion auf Bedrohungen** auf den Link **Verbindungseinstellungen** klicken. Führen Sie anschließend im angezeigten Bereich die folgenden Aktionen aus:

   a. Fügen Sie ein Serverzertifikat hinzu, indem Sie im entsprechenden Abschnitt auf die Schaltfläche **Hochladen** klicken.

   b. Wenn Sie zusätzlichen Schutz benötigen, erstellen Sie einen Crypto-Container.

      Gehen Sie dazu im Abschnitt **Zusätzlicher Verbindungsschutz** wie folgt vor:

      1. Aktivieren Sie das Kontrollkästchen **Zwei-Wege-Authentifizierung verwenden**.
      2. Klicken Sie auf die Schaltfläche **Hochladen** und fügen Sie das Client-Zertifikat hinzu, das Sie beim Abschluss des Hauptintegrationsszenarios erhalten haben.
      3. Geben Sie im entsprechenden Feld ein Kennwort für den Crypto-Container ein.

         Das Feld **Kennwort für Crypto-Container** ist erforderlich. Sie können die Einstellungen nicht speichern, ohne ein Kennwort für das Client-Zertifikat (Crypto-Container) einzugeben.
8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie die Integration von Kaspersky Endpoint Detection and Response Expert (on-premise) über die Befehlszeile

1. Um ein Zertifikat für den Response-Server hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type response
```

2. Um ein Zertifikat eines Servers zur Erfassung von Telemetriedaten hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type telemetry
```

3. Um die Integrationseinstellungen zu konfigurieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 24 [<setting name>=<setting value>]
```

Die Einstellungen und ihre möglichen Werte sind in der folgenden Tabelle aufgeführt.

4. Um ein Client-Zertifikat für die Verbindung mit dem Response-Server hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --add-kataedr-client-certificate <file> --server-type response
```

5. Um ein Client-Zertifikat für die Verbindung mit dem Server zur Erfassung von Telemetriedaten hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --add-kataedr-client-certificate <file> --server-type telemetry
```

6. Um die Integration mit EDR Expert (on-premise) zu aktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --start-task 24
```

Einstellungen der Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)

Parameter	Description	Wert
`Mode`	Modus der Integration. Bei der Integration in Kaspersky Endpoint Detection and Response Expert (on-premise) interagiert das Programm Kaspersky Endpoint Security mit Servern auf der OSMP-Plattform. Bei einer Integration mit Kaspersky Endpoint Detection and Response (KATA) kommuniziert Kaspersky Endpoint Security mit Servern auf der Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (Standardwert) – Integration im Modus EDR (KATA). Erlaubt die Integration mit Kaspersky Endpoint Detection and Response (KATA). Dies ist eine Komponente von Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` ist der Integrationsmodus EDR Expert (on-premise). Aktiviert die Integration in Kaspersky Endpoint Detection and Response Expert (on-premise)
`UseClientPinnedCertificate`	Aktivieren und Deaktivieren der Zwei-Wege-Authentifizierung, um die Verbindung zum OSMP-Reaktionsserver zusätzlich abzusichern. Wenn die Zwei-Wege-Authentifizierung aufseiten des OSMP-Servers für Bedrohungsreaktionen aktiviert ist, müssen Sie vor dem Start der Aufgabe die Zwei-Wege-Authentifizierung in den Einstellungen der Aufgabe *Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)* aktivieren und das Client-Zertifikat hinzufügen.	`Yes` aktiviert die Zwei-Wege-Authentifizierung, um die Verbindung zum OSMP-Server für Aktionen zur Reaktion auf Bedrohungen zusätzlich abzusichern. `No` (Standardwert) – Zwei-Wege-Authentifizierung nicht verwenden.
`SynchronizationPeriod`	Häufigkeit der Synchronisierungsanfragen an den OSMP-Reaktionsserver in Minuten.	Der Standardwert ist: `5`.
`ConnectionTimeout`	Maximale Wartezeit für eine Verbindung mit dem OSMP-Reaktionsserver in Sekunden.	Der Standardwert ist: `10`.
`RequestTimeout`	Maximale Wartezeit für eine Antwort vom OSMP-Reaktionsserver in Sekunden.	Der Standardwert ist: `10`.

Parameter	Description	Wert
`EnableTelemetry`	Senden von Daten zu Ereignissen auf Geräten (Telemetriedaten) an den OSMP-Server für die Erfassung von Telemetriedaten.	`Yes` (Standardwert) – Telemetriedaten an den OSMP-Telemetrieserver senden `No` – keine Telemetriedaten senden
Der Abschnitt **[Endpoints.item_#]** enthält die Adresse und den Port des OSMP-Reaktionsservers. Sie können mehrere Server hinzufügen.		
`Address`	Adresse des OSMP-Reaktionsservers Sie können die IP-Adresse (IPv4 oder IPv6) oder den vollqualifizierten Domänennamen (FQDN) des Servers angeben. Um sicherzustellen, dass die Kommunikation mit dem Server nicht unterbrochen wird, wenn die Anwendung bei aktivierter Netzwerkisolation des Geräts ausfällt, wird es empfohlen, die IP-Adresse des Servers anzugeben.	Der Standardwert ist: `127.0.0.1`.
`Port`	Der Port für die Verbindung zum OSMP-Reaktionsserver.	Der Standardwert ist: `443`.
Der Abschnitt **[TelemetrySettings]** enthält die allgemeinen Parameter zur Verbindung mit den OSMP-Telemetrieservern.		
`UseClientPinnedCertificate`	Aktivieren und Deaktivieren der Zwei-Wege-Authentifizierung, um die Verbindung zum OSMP-Telemetrieserver zusätzlich abzusichern. Wenn die Zwei-Wege-Authentifizierung aufseiten des OSMP-Telemetrieservers aktiviert ist, müssen Sie vor dem Start der Aufgabe die Zwei-Wege-Authentifizierung in den Einstellungen der Aufgabe *Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)* aktivieren und das Client-Zertifikat hinzufügen.	`Yes` aktiviert die Zwei-Wege-Authentifizierung, um die Verbindung zum OSMP-Telemetrieserver zusätzlich abzusichern. `No` (Standardwert) – Zwei-Wege-Authentifizierung nicht verwenden.
`ConnectionTimeout`	Maximale Wartezeit für eine Verbindung mit dem OSMP-Telemetrieserver in Sekunden.	Der Standardwert ist: `10`.
`RequestTimeout`	Maximale Wartezeit für eine Antwort vom OSMP-Telemetrieserver in Sekunden.	Der Standardwert ist: `10`.
`OnlyTaggedEvents`	Senden von Telemetriedaten nur mit IOA. Ein *Angriffsindikator (IOA)* ist eine Regel, die ein verdächtiges Verhalten im System beschreibt. Solches Verhaltens kann auf einen gezielten Angriff hinweisen. Das Programm vergleicht das aktuelle Verhalten im System mit diesen Regeln und protokolliert Ereignisse, die auf einen gezielten Angriff hindeuten. Das Programm verwendet die Technologie *Streaming-Scan*, um solche Ereignisse in Echtzeit zu verfolgen.	`Yes` – Nur Telemetriedaten senden, die mit einem Angriffsindikator versehen sind (Indicator of Attack, IOA) `No` (Standardwert) – Alle Telemetriedaten senden.
Der Abschnitt **[TelemetrySettings.Endpoints.item_#]** enthält die Adresse und den Port des OSMP-Telemetrieservers. Sie können mehrere Server hinzufügen.		
`Address`	Adresse des OSMP-Telemetrieservers. Sie können die IP-Adresse (IPv4 oder IPv6) oder den vollqualifizierten Domänennamen (FQDN) des Servers angeben. Um sicherzustellen, dass die Kommunikation mit dem Server nicht unterbrochen wird, wenn die Anwendung 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 OSMP-Telemetrieserver.	Der Standardwert ist: `443`.
Der Abschnitt **[TelemetrySettings.EventTransferSettings]** enthält die Parameter für die Datenübertragung an den OSMP-Telemetrieserver.		
`MaximumDataTransferTime`	Maximale Verzögerung beim Senden von Ereignissen an den OSMP-Telemetrieserver in Sekunden.	Der Standardwert ist: `30`.
`UseRequestCountLimits`	Begrenzen Sie die Anzahl der Anfragen. Durch diese Funktion wird die Auslastung des Computers optimiert. Wenn diese Funktion aktiviert ist, beschränkt die App die übertragenen Ereignisse. Wenn die Anzahl der Ereignisse die festgelegten Grenzwerte überschreitet, beendet Kaspersky Endpoint Security das Senden von Ereignissen.	`Yes` (Standardwert) – die Anzahl der gesendeten Ereignisse wird begrenzt `No` – die Anzahl der gesendeten Ereignisse wird nicht begrenzt
`MaximumNumberOfEventsInHour`	Maximale Anzahl an Ereignissen pro Stunde	Der Standardwert ist: `3000`.

Parameter	Description	Wert
`MaximumNumberOfEventsInPackage`	Die maximale Anzahl von Ereignissen in einem Paket.	Der Standardwert ist: `1024`.
`EventLimitExceededPercentage`	Prozentuale Überschreitung der Beschränkung der Ereignisanzahl: 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`.

Bei den Einstellungen für die Integration von Kaspersky Endpoint Detection and Response Expert (on-premise) ermöglichen in der Hierarchie verschachtelte Richtlinien die Angabe unabhängiger Werte, selbst wenn alle anderen Richtlinieneinstellungen vererbt werden.

Wenn die Integration von Kaspersky Endpoint Detection and Response Expert (on-premise) in der übergeordneten Richtlinie aktiviert ist und die Vererbung von Einstellungen in der untergeordneten Richtlinie aktiviert ist, werden standardmäßig auch die Integrationseinstellungen der untergeordneten Richtlinie vererbt und können nicht geändert werden. Wenn Sie unabhängige Integrationseinstellungen konfigurieren möchten, wählen Sie in der Dropdown-Liste **Benutzerdefinierte Verbindungseinstellungen verwenden** aus. Dadurch können die Einstellungen für die Integration von Kaspersky Endpoint Detection and Response Expert (on-premise) bearbeitet werden.

Wenn Sie die Web Console oder die Befehlszeile verwenden, müssen Sie für die Integration mit Kaspersky Endpoint Detection and Response (on-premise) in den Einstellungen der Komponente EDR Expert (on-premise) den Integrationsmodus EDR (on-premise) auswählen:

- Wenn Sie die Web Console verwenden, wählen Sie in den Richtlinieneigenschaften die Option **Endpoint Detection and Response Expert (Version 8.0 und höher)** aus. Um die Integration von Kaspersky Endpoint Detection and Response (on-premise) auf einem Gerät zu konfigurieren, müssen Sie in der Web Console für eine der Versionen (Version 8.0 und höher oder Version 7.1 und früher) die „Schlösser“ verwalten.
- Wenn Sie die Befehlszeile verwenden, geben Sie in den Aufgabeneinstellungen den Parameter `Mode=EDRExpertOnPrem` an.

So überprüfen Sie, ob die Integration in EDR Expert (on-premise) betriebsbereit ist

So testen Sie die Komponente „EDR Expert (on-premise)“:

- Über die Befehlszeile mit folgendem Befehl:

```
kesl-control --app-info
```

- In der Web Console.
  - Berichte in der Kaspersky Security Center-Konsole:

    Mithilfe des *Berichts über den Status der Programmkomponenten*. Weitere Informationen zum Umgang mit Berichten finden Sie in der Hilfe zu Kaspersky Security Center.
  - In der OSMP-Konsole:
    - Mithilfe des *Berichts über den Status der Programmkomponenten*.
    - Wechseln Sie zum Abschnitt **Asset-Management** → **Assets** und wählen Sie die Registerkarte **Analyse und Reaktion** aus.

      Das Gerät wird in der Liste mit dem Status der Telemetriedaten **Normale Aktivität** angezeigt.

- Gehen Sie zum Abschnitt **Bedrohungssuche**.

  Telemetriedatenereignisse vom Gerät werden in der Liste der Ereignisse angezeigt.

Endpoint Detection and Response Expert (cloud)

Die Integration von Kaspersky Endpoint Security für Linux in Kaspersky Endpoint Detection and Response Expert (cloud) ist vorübergehend nicht verfügbar. Diese Funktionalität wird planmäßig bis Ende 2026 unterstützt. Bitte beachten Sie unsere Versionshinweise. Dort finden Sie aktuelle Informationen über Programm-Upgrades und neue Funktionen.

Kaspersky Endpoint Security für Linux unterstützt die Integration in die Lösung Kaspersky Endpoint Detection and Response Expert (cloud). *Kaspersky Endpoint Detection and Response Expert (cloud)* ist eine Cybersicherheitslösung für Unternehmen. Mit den darin enthaltenen Kaspersky-Anwendungen kann sich ein Unternehmen vor den meisten Arten von Cyber-Risiken schützen und die wichtigsten Verbreitungsszenarien für Bedrohungen abdecken. Die Komponenten von EDR Expert (cloud) werden auf der Open Single Management Platform (OSMP) bereitgestellt. Diese Plattform führt plattformübergreifende Szenarien auf einer einzigen Benutzeroberfläche aus und ermöglicht die Integration von Kaspersky-Programmen in Dritthersteller-Programme, um ein umfassendes Sicherheitssystem zu gestalten.

Eines der zentralen Elemente dieser Lösung ist *SIEM*. SIEM verfolgt Ereignisse, die von allen Komponenten stammen, und stellt mithilfe von Herstellerregeln und benutzerdefinierten Regeln Zusammenhänge zwischen diesen Ereignissen her. EDR Expert (cloud) analysiert von der Unternehmensinfrastruktur empfangene Protokolle und Telemetriedaten, um Angriffe automatisch zu erkennen, und ermöglicht die Untersuchung von Vorfällen. Dazu dient ein einheitlicher Untersuchungsgraph, der alle in EDR Expert (cloud) erfassten Ereignisse kombiniert, einschließlich der Ereignisse aus Kaspersky-Anwendungen und Drittanbieter-Sicherheitsprodukten.

Zur Reaktion auf komplexe Vorfälle verwendet EDR Expert (cloud) vordefinierte und benutzerdefinierte Szenarien. Sie können auch Reaktionen aus Drittanbieter-Programmen sowie Reaktionsszenarien verwenden, an denen mehrere Programme beteiligt sind.

Threat Intelligence-Tools

Kaspersky Endpoint Detection and Response verwendet die folgenden Threat Intelligence-Tools:

- Integration in Kaspersky Threat Intelligence Portal, das Informationen über die Reputation von Dateien und Webadressen enthält und anzeigt.
- Die Bedrohungsdatenbank Kaspersky Threats von Kaspersky.
- Die Cloud-Service-Infrastruktur von Kaspersky Security Network (im Folgenden auch „KSN“ genannt), die Echtzeitzugriff auf Datei-, Website- und Software-Reputationsinformationen aus der Kaspersky-Wissensdatenbank bietet. Durch die Verwendung von Daten aus Kaspersky Security Network wird die Reaktion der Kaspersky-Programme auf Bedrohungen beschleunigt und die Leistungsfähigkeit bestimmter Schutzkomponenten erhöht. Außerdem verringert sich das Risiko von Fehlalarmen.

Funktionsweise der Lösung

Kaspersky Endpoint Security wird auf den einzelnen Computern einer IT-Unternehmensinfrastruktur installiert und überwacht kontinuierlich Prozesse, offene Netzwerkverbindungen und geänderte Dateien.

Informationen über Ereignisse auf dem Computer (Telemetrie) werden an den Server von EDR Expert (cloud) gesendet. In diesem Fall sendet Kaspersky Endpoint Security an die Telemetrie-Erfassungsserver auch Informationen über die vom Programm erkannten Bedrohungen sowie Informationen über die Verarbeitungsergebnisse dieser Bedrohungen.

Die Integration von EDR Expert (cloud) wird in der Kaspersky Security Center-Konsole konfiguriert. Anschließend wird der integrierte Agent über Open Single Management Platform (OSMP) verwaltet. Dies bezieht sich beispielsweise auch auf folgende Vorgänge: Aufgaben ausführen, Objekte in der Quarantäne verwalten und Berichte anzeigen.

Einschränkungen von EDR Expert (cloud)

- Kaspersky Endpoint Security unterstützt die Integration mit EDR Expert (cloud) im Light Agent-Modus nicht.
- EDR Expert (cloud) ist für Geräte mit einer Elbrus-CPU nicht verfügbar.
- EDR Expert (cloud) wird auf Geräten mit Arm-Architektur nicht unterstützt.
- EDR Expert (cloud) ist für Computer mit 64-Bit-Betriebssystemen nicht verfügbar.

So konfigurieren Sie die Integration des integrierten Agenten in EDR Expert (cloud)

Für die Integration in die Lösung Kaspersky Endpoint Detection and Response Expert (cloud) müssen Sie die Komponente Endpoint Detection and Response Expert (cloud) aktivieren und die Verbindung zum Server zur Erfassung von Telemetriedaten und zum Reaktionsserver konfigurieren.

Ein *Telemetrie-Erfassungsserver* ist Teil einer SIEM-Lösung, die Informationen über auf dem Computer auftretende Ereignisse sammelt, normalisiert, korreliert, analysiert und speichert.

Ein *Reaktionsserver* ist ein Server, der Daten empfängt und sendet, das Verhalten von Objekten analysiert und die Ergebnisse solcher Untersuchungen veröffentlicht.

> Die Komponenten *Endpoint Detection and Response (cloud)* und *Endpoint Detection and Response Expert (on-premise)* sind nicht miteinander kompatibel.

Betriebsbedingungen für EDR Expert (cloud)

Damit EDR Expert (cloud) funktioniert, müssen die folgenden Bedingungen erfüllt sein:

- Die Infrastruktur von Kaspersky Endpoint Detection and Response Expert (cloud) ist in Ihrer Region verfügbar. Informationen zur Verfügbarkeit der Infrastruktur von EDR Expert (cloud) in Ihrer Region erhalten Sie beim Technischen Support.
- OSMP (Open Single Management Platform) ist installiert.
- Kaspersky Endpoint Security im Standardmodus installiert.
- Kaspersky Endpoint Security ist aktiviert und die Funktionalität ist durch die Lizenz abgedeckt.
- Sie haben die Bedingungen der Vereinbarung zur Datenverarbeitung für Kaspersky Endpoint Detection and Response Expert (cloud) akzeptiert.
- Die Komponente Endpoint Detection and Response Expert (cloud) ist aktiviert.
- Die Komponente Verhaltensanalyse zur Übertragung der erforderlichen Telemetriedaten ist aktiviert.

  Wenn Sie Informationen über erkannte Bedrohungen von anderen Schutzkomponenten erhalten möchten, aktivieren Sie diese Komponenten:

  - Schutz vor bedrohlichen Dateien.
  - Schutz vor Netzwerkbedrohungen.
  - Schutz vor Web-Bedrohungen.
  - Schutz vor Verschlüsselung.
  - Programmkontrolle.
  - Gerätekontrolle.
  - Überwachung der Systemintegrität.

Schritte zur Integration mit EDR Expert (cloud)

Die Einrichtung der Integration für EDR Expert (cloud) umfasst die folgenden Schritte:

1. **Auswählen eines EDR Expert-Modus**

   Kaspersky Endpoint Security unterstützt zwei EDR Expert-Modi: on-premise und cloud. Für die Integration in Kaspersky Endpoint Detection and Response Expert (cloud) müssen Sie während der Installation des Programms den entsprechenden Modus aktivieren. Standardmäßig verwendet das Programm die Integration mit Endpoint Detection and Response Expert (on-premise).

2. **Kaspersky Endpoint Detection and Response Expert (cloud) aktivieren**

   Sie müssen eine separate Lizenz für Kaspersky Endpoint Detection and Response Expert (cloud) kaufen.

Die Funktionalität ist verfügbar, sobald ein separater Schlüssel für Kaspersky Endpoint Detection and Response (cloud) hinzugefügt wurde. Dadurch werden zwei Schlüssel auf dem Computer hinzugefügt: ein Schlüssel für Kaspersky Endpoint Security und ein Schlüssel für Kaspersky Endpoint Detection and Response (cloud).

Die Lizenzierung der eigenständigen Funktionalität von Endpoint Detection and Response (cloud) entspricht der Lizenzierung von Kaspersky Endpoint Security.

Stellen Sie sicher, dass die Funktionalität von EDR Expert (cloud) von Ihrer Lizenz abgedeckt ist und in Kaspersky Security Center oder auf dem geschützten Gerät funktioniert.

3 Konfigurieren der Verbindung zum Server zur Erfassung von Telemetriedaten und zum Reaktionsserver

Kaspersky Endpoint Detection and Response Expert (cloud) erfordert eine vertrauenswürdige Verbindung zwischen Kaspersky Endpoint Security und zwei Servern: dem Server zur Erfassung von Telemetriedaten und dem Reaktionsserver. Das Programm erhält Serveradressen und Zertifikate zum Herstellen einer vertrauenswürdigen Verbindung automatisch, nachdem Sie die Bedingungen der Vereinbarung zur Datenverarbeitung von Kaspersky Endpoint Detection and Response Expert (cloud) akzeptiert haben. Daher müssen Sie nur die erweiterten Einstellungen für die Verbindung mit den Servern verwalten: ob Sie einen TCP-Tunnel verwenden möchten und in welchem Intervall eine Anfrage zur Synchronisierung mit dem Server gesendet werden soll.

So konfigurieren Sie zusätzliche Einstellungen für die Verbindung von Kaspersky Endpoint Security mit EDR Expert (cloud) in der Web Console

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response Expert (Cloud)**.
5. Aktivieren Sie die Komponente mithilfe des Schalters **Endpoint Detection and Response Expert (Cloud) DEAKTIVIERT**.
6. Wenn die aktuelle Richtlinie eine untergeordnete Richtlinie ist und die übergeordnete Richtlinie Änderungen an den Integrationseinstellungen für EDR Expert (cloud) untersagt (geschlossenes „Vorhängeschloss"), können Sie die Vererbung von Einstellungen im Abschnitt **Vererbung** konfigurieren:

   - **Verbindungseinstellungen aus der Richtlinie übernehmen** (Standardwert). Die Verbindungseinstellungen werden von der übergeordneten Richtlinie vererbt. Sie können die Einstellungen nicht ändern.
   - **Benutzerdefinierte Verbindungseinstellungen verwenden**. Sie können die Verbindungseinstellungen manuell konfigurieren.
7. Auf der Registerkarte **Reaktionsserver** werden der vollständig qualifizierte Domänenname und der Port des Reaktionsservers angezeigt, die automatisch abgerufen werden. Wenn die Sicherheitsrichtlinie in Ihrer Infrastruktur keine direkte Verbindung mit Servern von EDR Expert (cloud) zulässt, können Sie eine Verbindung über einen TCP-Tunnel einrichten:

   a. Aktivieren Sie das Kontrollkästchen **TCP-Tunnel für die Reaktion verwenden**.

   b. Geben Sie die Serveradresse (IPv4, IPv6) und den Port für die Tunnelverbindung an.

8. Legen Sie bei Bedarf im Feld **Synchronisierungsanfrage an Server senden alle (Min.)** fest, wie häufig Synchronisierungsanfragen an den Server gesendet werden sollen. Während der Synchronisierung empfängt Kaspersky Endpoint Security Aufgaben zur Reaktion auf Bedrohungen und sendet Aufgabenergebnisse.

9. Gehen Sie zur Registerkarte **Telemetrie-Erfassungsserver**.

10. Konfigurieren Sie die Verbindungseinstellungen für den Server zur Erfassung von Telemetriedaten:

    a. Klicken Sie auf den Link **Ändern**.

    b. Daraufhin wird ein Fenster geöffnet; wählen Sie in diesem Fenster einen Server zur Erfassung von Telemetriedaten aus der Liste aus. Der KUMA-Kollektor dient in EDR Expert (cloud) als Telemetrie-Erfassungsserver. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform.

    Falls beim Verbinden mit dem Telemetrie-Erfassungsserver ein Fehler auftritt, wählen Sie einen anderen Server aus. Wenn Sie keine Verbindung zum Server zur Erfassung von Telemetriedaten herstellen können, wenden Sie sich bitte an den Technischen Support.

    c. Bei Bedarf können Sie eine Verbindung zum Telemetrie-Erfassungsserver über einen TCP-Tunnel konfigurieren, genauso wie für den Reaktionsserver.

11. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So zeigen Sie Zertifikatsinformationen über die Befehlszeile an

1. Führen Sie den folgenden Befehl aus, um Informationen über ein Client-Zertifikat anzuzeigen:

```
kesl-control --query-cloudxdr-client-certificate --server-type telemetry
```

```
kesl-control --query-cloudxdr-client-certificate --server-type response
```

2. Führen Sie den folgenden Befehl aus, um Informationen über ein Server-Zertifikat anzuzeigen:

```
kesl-control --query-cloudxdr-server-certificate --server-type telemetry
```

```
kesl-control --query-cloudxdr-server-certificate --server-type response
```

Daraufhin zeigt Kaspersky Endpoint Security die Zertifikatsinformationen wie folgt an:

```
Serial number: 12 34 56 78 AB CD EF GH
Subject: C=EN, ST=Moscow, L=Moscow, O=AO Kaspersky Lab, OU=Future Technologies, CN=epp
Issuer: C=EN, ST=Moscow, L=Moscow, O=AO Kaspersky Lab, OU=Future Technologies, CN=epp
Valid from: 2022-07-27 13:25:35
Expires on: 2072-07-14 13:25:35
SHA1 fingerprint: a14f12df23fg3465bgh6345g567df
```

Überprüfen Sie den Betriebsstatus der Komponente, indem Sie sich den *Bericht über den Status der Programmkomponenten* ansehen. Sie können auch den Status der Komponente auf dem geschützten Gerät anzeigen.

So optimieren Sie die Übertragung von Telemetriedaten in EDR Expert (cloud)

Telemetrie ist eine Liste von Ereignissen, die auf dem geschützten Computer aufgetreten sind. Kaspersky Endpoint Security analysiert Telemetrie-Daten und sendet diese während der Synchronisierung an Telemetrie-Erfassungsserver. Telemetrie-Ereignisse treffen fast kontinuierlich auf dem Server ein. Kaspersky Endpoint Security startet die Synchronisierung mit dem Server, wenn eine der folgenden Bedingungen erfüllt ist:

- Das Synchronisierungsintervall ist abgelaufen.
- Die Anzahl der Ereignisse im Puffer überschreitet die Höchstgrenze.

Dann synchronisiert die App standardmäßig alle 30 Sekunden oder immer, wenn der Puffer 1024 Ereignisse enthält. Sie können das Synchronisierungsverhalten in der Richtlinie von Kaspersky Endpoint Security anpassen und optimale Werte für Ihre Netzwerklast auswählen (siehe Anleitung unten).

Bei fehlender Verbindung zwischen Kaspersky Endpoint Security und dem Server stellt die App neue Ereignisse in die Warteschlange. Sobald die Verbindung wiederhergestellt wird, sendet Kaspersky Endpoint Security die Ereignisse aus der Warteschlange in der richtigen Reihenfolge an den Server. Um eine Überlastung des Servers zu vermeiden, kann Kaspersky Endpoint Security bestimmte Ereignisse überspringen. Diese Option können Sie in den Einstellungen für die Ereignisübertragung optimieren und dafür beispielsweise einen Höchstwert für Ereignisse pro Stunde festlegen (siehe Anleitung unten).

So optimieren Sie die Übertragung von Telemetriedaten in der Web Console

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response Expert (Cloud)**.
5. Wählen Sie im folgenden Fenster die Registerkarte **Einstellungen für die Datenübertragung** aus.
6. Stellen Sie sicher, dass das Kontrollkästchen **Telemetrie-Übertragung AKTIVIERT** aktiviert ist.
7. Aktivieren Sie bei Bedarf die Funktion **Telemetrie nur mit IOA senden**. Ein *Angriffsindikator (IOA)* ist eine Regel, die ein verdächtiges Verhalten im System beschreibt. Solches Verhaltens kann auf einen gezielten Angriff hinweisen. Das Programm vergleicht das aktuelle Verhalten im System mit diesen Regeln und protokolliert Ereignisse, die auf einen gezielten Angriff hindeuten. Das Programm verwendet die Technologie *Streaming-Scan*, um solche Ereignisse in Echtzeit zu verfolgen. Die Funktion ist standardmäßig deaktiviert.
8. Passen Sie bei Bedarf die Einstellungen für die Serversynchronisierung an:
   - **Maximale Verzögerung der Ereignisübertragung (Sek.)**. Die App synchronisiert sich mit dem Server, um Ereignisse nach Ablauf des Synchronisierungsintervalls zu senden. Der Standardwert ist 30 Sekunden.
   - **Maximale Anzahl der Ereignispakete**. Das Programm synchronisiert sich mit dem Server, wenn sich genügend Ereignisse im Puffer befinden. Der Standardwert beträgt 1.024 Ereignisse.
9. Gehen Sie zur Registerkarte **Anforderungsbegrenzung**.

10. Deaktivieren Sie bei Bedarf die Anforderungsbegrenzung mithilfe des Umschalters **Anforderungsbegrenzung AKTIVIERT**.

    Durch diese Funktion wird die Auslastung des Computers optimiert. Wenn diese Funktion aktiviert ist, beschränkt die App die übertragenen Ereignisse. Wenn die Anzahl der Ereignisse die festgelegten Grenzwerte überschreitet, beendet Kaspersky Endpoint Security das Senden von Ereignissen. Diese Option ist standardmäßig deaktiviert.

11. Konfigurieren Sie die Optimierungseinstellungen für das Senden von Ereignissen an den Server:

    - **Maximale Anzahl von Ereignissen pro Stunde**. Die App analysiert den Telemetriedatenstrom und schränkt das Senden von Ereignissen ein, wenn der Ereignisstrom das festgelegte Limit für Ereignisse pro Stunde überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen nach einer Stunde fort. Die Standardeinstellung ist 3.000 Ereignisse pro Stunde. Wenn die App auf einem Server installiert ist, ist der Telemetrie-Datenstrom höher. Für Server wird empfohlen, den Wert auf 60.000 Ereignisse pro Stunde zu erhöhen.

    - **Prozentsatz für die Überschreitung des Ereignislimits (%)**. Die App sortiert Ereignisse nach Typ (z. B. Ereignisse des Typs „Änderungen in der Registrierung“) und schränkt die Übertragung von Ereignissen ein, wenn das Verhältnis von Ereignissen desselben Typs zur Gesamtzahl von Ereignissen den in Prozent festgelegten Grenzwert überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen fort, wenn das Verhältnis der anderen Ereignisse zur Gesamtzahl der Ereignisse wieder dem Grenzwert entspricht. Die Standardeinstellung ist 15%.

12. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So optimieren Sie die Übertragung von Telemetriedaten über die Befehlszeile

1. Um das Senden von Telemetriedaten zu aktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 39 [EnableTelemetry=<Yes|No>] [TelemetrySettings.OnlyTaggedEvents=<Yes|No>]
```

2. Führen Sie den folgenden Befehl aus, um die Synchronisierungseinstellungen mit dem Server anzupassen:

```
kesl-control --set-settings 39 [TelemetrySettings.EventTransferSettings.UseRequestCountLimits=<Yes|No>]
[TelemetrySettings.EventTransferSettings.MaximumDataTransferTime=<delay in sending events in seconds>]
[TelemetrySettings.EventTransferSettings.MaximumNumberOfEventsInHour=<number of events>]
[TelemetrySettings.EventTransferSettings.MaximumNumberOfEventsInPackage=<number of event packages>]
[TelemetrySettings.EventTransferSettings.EventLimitExceededPercentage=<percentage of exceeding the event
limit>]
```

Integrationseinstellungen für Kaspersky Endpoint Detection and Response Expert (cloud)

Parameter	Description
`EnableTelemetry`	Senden von Daten zu Ereignissen auf Geräten (Telemetriedaten) an den OSMP-Server für die Erfassung von Telemetriedaten. Das Senden von Telemetriedaten ist standardmäßig aktiviert (`Yes`).
`TelemetrySettings.OnlyTaggedEvents`	Senden von Telemetriedaten nur mit IOA. Ein *Angriffsindikator (IOA)* ist eine Regel, die ein verdächtiges Verhalten im System beschreibt. Solches Verhaltens kann auf einen gezielten Angriff hinweisen. Das Programm vergleicht das aktuelle Verhalten im System mit diesen Regeln und protokolliert Ereignisse, die auf einen gezielten Angriff hindeuten. Das Programm verwendet die Technologie *Streaming-Scan*, um solche Ereignisse in Echtzeit zu verfolgen. Standardmäßig ist das Senden von Telemetriedaten nur mit IOA deaktiviert (`No`).
Der Abschnitt `[TelemetrySettings.EventTransferSettings]` enthält allgemeine Einstellungen für die Verbindung mit OSMP-Telemetrieservern.	

Parameter	Description
`UseRequestCountLimits`	Anforderungsbegrenzung. Durch diese Funktion wird die Auslastung des Computers optimiert. Wenn diese Funktion aktiviert ist, beschränkt die App die übertragenen Ereignisse. Wenn die Anzahl der Ereignisse die festgelegten Grenzwerte überschreitet, beendet Kaspersky Endpoint Security das Senden von Ereignissen. Diese Option ist standardmäßig deaktiviert.
`MaximumDataTransferTime`	Maximale Verzögerung der Ereignisübertragung (Sek.). Die App synchronisiert sich mit dem Server, um Ereignisse nach Ablauf des Synchronisierungsintervalls zu senden. Der Standardwert ist 30 Sekunden.
`MaximumNumberOfEventsInHour`	Maximale Anzahl von Ereignissen pro Stunde. Die App analysiert den Telemetriedatenstrom und schränkt das Senden von Ereignissen ein, wenn der Ereignisstrom das festgelegte Limit für Ereignisse pro Stunde überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen nach einer Stunde fort. Die Standardeinstellung ist 3.000 Ereignisse pro Stunde. Wenn die App auf einem Server installiert ist, ist der Telemetrie-Datenstrom höher. Für Server wird empfohlen, den Wert auf 60.000 Ereignisse pro Stunde zu erhöhen.
`MaximumNumberOfEventsInPackage`	Maximale Anzahl an Ereignissen pro Paket Das Programm synchronisiert sich mit dem Server, wenn sich genügend Ereignisse im Puffer befinden. Der Standardwert beträgt 1.024 Ereignisse.
`EventLimitExceededPercentage`	Prozentsatz für die Überschreitung des Ereignislimits (%). Die App sortiert Ereignisse nach Typ (z. B. Ereignisse des Typs „Änderungen in der Registrierung“) und schränkt die Übertragung von Ereignissen ein, wenn das Verhältnis von Ereignissen desselben Typs zur Gesamtzahl von Ereignissen den in Prozent festgelegten Grenzwert überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen fort, wenn das Verhältnis der anderen Ereignisse zur Gesamtzahl der Ereignisse wieder dem Grenzwert entspricht. Die Standardeinstellung ist 15%.

So konfigurieren Sie Ausnahmen für Telemetriedaten in EDR Expert (cloud)

Um die Leistung zu verbessern und die Datenübertragung an den Telemetrie-Erfassungsserver zu optimieren, können Sie Telemetrie-Ausnahmen hinzufügen. Sie können beispielsweise festlegen, dass für einzelne Anwendungen keine Netzwerkkommunikationsdaten gesendet werden.

Wenn zu viele Regeln verwendet werden, kann sich die Auslastung des Servers für die Erfassung von Telemetriedaten erhöhen und die Computerleistung verringern. Es wird empfohlen, nur erforderlich Regeln hinzuzufügen.

So erstellen Sie eine Ausnahme für Telemetriedaten in der Web Console:

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Telemetrie-Einstellungen**.
5. Wählen Sie die Registerkarte **Telemetrie für EDR Expert (Cloud)** aus.
6. Klicken Sie im Block **Allgemeine Ausnahmen** auf **Hinzufügen**.
   Dadurch wird ein Fenster zum Hinzufügen einer Regel für Telemetriedaten-Ausnahmen geöffnet.

7. Konfigurieren Sie die Regel für Telemetriedaten-Ausnahmen:

   a. Ändern Sie bei Bedarf den Status der Regel. Die Regel ist standardmäßig aktiviert.

   b. Geben Sie einen Namen für die Regel ein.

   c. Wählen Sie die Aktion aus, die bei Auslösung der Regel ausgeführt werden soll:

      - **Nicht sammeln**. Das gefilterte Ereignis wird aus den zu sendenden Telemetriedaten ausgeschlossen.

      - **IOA ausschließen**. Das Trigger-Ereignis der IOA-Regel wird aus den zu sendenden Telemetriedaten ausgeschlossen. Ein *Angriffsindikator (IOA)* ist eine Regel, die ein verdächtiges Verhalten im System beschreibt. Solches Verhaltens kann auf einen gezielten Angriff hinweisen. Das Programm vergleicht das aktuelle Verhalten im System mit diesen Regeln und protokolliert Ereignisse, die auf einen gezielten Angriff hindeuten. Das Programm verwendet die Technologie *Streaming-Scan*, um solche Ereignisse in Echtzeit zu verfolgen.

   d. Wenn die Option **IOA ausschließen** ausgewählt ist, geben Sie an, welche IOA-Regeln zu den Ausnahmen hinzugefügt werden sollen:

      - **Alle ausschließen**. Wenn die angegebene Bedingung erfüllt ist, werden die Ereignisse, die basierend auf allen IOA-Regeln generiert wurden, von der Telemetrie ausgeschlossen.

      - **Nach GUID ausschließen**. Geben Sie die GUID der IOA-Regel an. Sie können mehrere GUIDs durch `,` getrennt angeben. Details über die IOA-Regeln finden Sie in der Hilfe zu EDR Expert (cloud).

   e. Geben Sie die Filterbedingungen an:

   Bei Bedarf können Sie komplexe Filterkriterien erstellen, indem Sie mithilfe der Operatoren **UND**, **ODER** und **NICHT** mehrere Filterbedingungen und Bedingungsgruppen hinzufügen. Sie können einer Bedingungsgruppe auch verschachtelte Bedingungen und Bedingungsgruppen hinzufügen.

8. Fügen Sie bei Bedarf unter **Alle Ereignistypen** Telemetrie-Ausnahmen hinzu, die vom Ereignistyp abhängen.

   a. Klicken Sie auf den Namen des Ereignistyps.

   b. Klicken Sie im angezeigten Fenster auf **Manuell einrichten**.

   c. Klicken Sie im Block **Ausschlussregeln** auf **Hinzufügen**.

      Dadurch wird ein Fenster zum Hinzufügen einer Regel für Telemetriedaten-Ausnahmen geöffnet. In der Regel für Telemetriedaten-Ausnahmen ist die Filterbedingung `EventType`, die dem Ereignistyp entspricht, bereits voreingestellt.

   d. Geben Sie die Filterbedingungen an:

9. Um die Richtlinie auf Computer anzuwenden, vergewissern Sie sich, dass die Vorhängeschlösser geschlossen sind (🔒), und speichern Sie Ihre Änderungen.

So exportieren oder importieren Sie Ereignisfilter für EDR Expert (cloud)

Sie können die Ausnahmeliste in eine json-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Ereignis-IDs hinzuzufügen. Sie können die Export-/Importfunktion auch verwenden, um ein Backup der Ereignisfilter anzulegen oder die Listen auf einen anderen Server zu migrieren.

Wenn zu viele Regeln verwendet werden, kann sich die Auslastung des Servers für die Erfassung von Telemetriedaten erhöhen und die Computerleistung verringern. Es wird empfohlen, nur erforderlich Regeln hinzuzufügen.

So exportieren oder importieren Sie Ereignisfilter (in der Web Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Telemetrie-Einstellungen**.
5. Wählen Sie die Registerkarte **Telemetrie für EDR Expert (Cloud)** aus.
6. So exportieren Sie die Ereignisfilter:
   a. Klicken Sie auf **Exportieren**.
   b. Geben Sie im folgenden Fenster den Namen der json-Datei an, in die Sie die Ereignisfilter exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   c. Speichern Sie die Datei.

      Kaspersky Endpoint Security exportiert die Ereignisfilter in die json-Datei.
7. So importieren Sie Ereignisfilter:
   a. Klicken Sie auf **Import**.
   b. Wählen Sie im folgenden Fenster die json-Datei aus, aus der Sie die Ereignisfilter importieren möchten.
   c. Wählen Sie aus, auf welche Weise die Regeln für die Ereignisfilterung importiert werden sollen: Regeln zu vorhandenen Regeln hinzufügen oder vorhandene Regeln verwerfen und durch neue ersetzen.
   d. Öffnen Sie die Datei.
8. Um die Richtlinie auf Computer anzuwenden, vergewissern Sie sich, dass die Vorhängeschlösser geschlossen sind (🔒), und speichern Sie Ihre Änderungen.
   1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
   2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

      Das Eigenschaftenfenster der Richtlinie wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Allgemeine Einstellungen** → **Telemetrie-Einstellungen**.

5. Wählen Sie die Registerkarte **Telemetrie für EDR Expert (Cloud)** aus.

6. So exportieren Sie die Ereignisfilter:

   a. Klicken Sie auf **Exportieren**.

   b. Geben Sie im folgenden Fenster den Namen der json-Datei an, in die Sie die Ereignisfilter exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   c. Speichern Sie die Datei.

   Kaspersky Endpoint Security exportiert die Ereignisfilter in die json-Datei.

7. So importieren Sie Ereignisfilter:

   a. Klicken Sie auf **Import**.

   b. Wählen Sie im folgenden Fenster die json-Datei aus, aus der Sie die Ereignisfilter importieren möchten.

   c. Wählen Sie aus, auf welche Weise die Regeln für die Ereignisfilterung importiert werden sollen: Regeln zu vorhandenen Regeln hinzufügen oder vorhandene Regeln verwerfen und durch neue ersetzen.

   d. Öffnen Sie die Datei.

8. Um die Richtlinie auf Computer anzuwenden, vergewissern Sie sich, dass die Vorhängeschlösser geschlossen sind (🔒), und speichern Sie Ihre Änderungen.

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform ist eine Lösung zum Schutz der IT-Infrastruktur eines Unternehmens und zur frühzeitigen Erkennung von Bedrohungen wie Zero-Day-Angriffen, gezielten Angriffen und Advanced Persistent Threats (im Folgenden auch APT genannt). Einzelheiten über diese Lösung finden Sie in der Hilfe zu „Kaspersky Anti Targeted Attack Platform“.

Kaspersky Endpoint Security kann mit den folgenden Komponenten auf Basis der Kaspersky Anti Targeted Attack Platform integriert werden:

Kaspersky Endpoint Detection and Response (KATA)

Die Komponente gewährleistet den Schutz für Geräte im lokalen Netzwerk der Organisation. Bei Integration mit Kaspersky Endpoint Detection and Response (KATA) führt Kaspersky Endpoint Security die folgenden Funktionen aus:

- Senden von Informationen über Ereignisse auf Geräten (Telemetriedaten) an den Central Node-Server, der die Interaktion mit Kaspersky Endpoint Detection and Response (KATA) ermöglicht (im Folgenden auch *KATA-Server* genannt).

  Kaspersky Endpoint Security sendet Überwachungsdaten zu Prozessen, offenen Netzwerkverbindungen und geänderten Dateien sowie Daten zu den von der Anwendung erkannten Bedrohungen und Daten zu den Verarbeitungsergebnissen dieser Bedrohungen an die Central Node-Komponente.

- Ausführen von Aktionen zur Reaktion auf Bedrohungen, um beim Empfang von Befehlen von Kaspersky Anti Targeted Attack Platform die Sicherheit zu gewährleisten.

Die Integration mit Kaspersky Endpoint Detection and Response (KATA) 7.1 und früheren Versionen wird unterstützt.

Network Detection and Response (KATA)

Diese Komponente gewährleistet den Schutz für das interne Netzwerk des Unternehmens. Bei Integration mit Kaspersky Endpoint Detection and Response (KATA) kann Kaspersky Endpoint Security Daten zu Ereignissen auf Geräten (Telemetriedaten) an einen Server mit Central-Node-Komponente senden, der die Interaktion mit Kaspersky Endpoint Detection and Response (KATA) ermöglicht (im Folgenden auch als *NDR-Server* bezeichnet).

Sandbox

Die Anwendung Kaspersky Endpoint Security sendet Dateien zur Untersuchung an den Central Node-Server, der für die Interaktion mit Sandbox zuständig ist.

Die folgenden Komponenten von Kaspersky Endpoint Security ermöglichen die Integration mit Kaspersky Anti Targeted Attack Platform:

- Endpoint Detection and Response Expert (on-premise), im Folgenden auch *EDR Expert (on-premise)* genannt.

  Ab Kaspersky Endpoint Security 12.4 für Linux wurde die Komponente Endpoint Detection and Response (KATA) in Endpoint Detection and Response Expert (on-premise) umbenannt. Jetzt ermöglicht diese Komponente die Integration nicht nur mit Kaspersky Endpoint Detection and Response (KATA), einer Komponente der Kaspersky Anti Targeted Attack Platform, sondern auch mit der Lösung Kaspersky Endpoint Detection and Response Expert (on-premise).

- Network Detection and Response (KATA), im Folgenden auch *NDR (KATA)* genannt.

- Sandbox.

Sie können die Integration der App Kaspersky Endpoint Security entweder mit allen Komponenten der Kaspersky Anti Targeted Attack Platform-Lösung oder mit jeder Komponente separat konfigurieren.

Die Komponente ist für Geräte mit Elbrus-CPU nicht verfügbar.

Integration mit Kaspersky Anti Targeted Attack Platform konfigurieren

Voraussetzungen

Bevor Sie die Integration mit Kaspersky Network Detection and Response (KATA) konfigurieren, erlauben Sie Verbindungen über Port 8085.

Bevor Sie die Integration mit der Komponente Kaspersky Endpoint Detection and Response (KATA) konfigurieren:

- Erlauben Sie Verbindungen über die Ports 443 und 8443.
- Aktivieren Sie die Komponente Verhaltensanalyse, um die erforderlichen Telemetriedaten zu übertragen.

  Die Komponente Verhaltensanalyse ist auf Geräten mit Kernel-Version 3.13 und höher verfügbar.

  Wenn Sie Informationen über erkannte Bedrohungen von anderen Schutzkomponenten erhalten möchten, aktivieren Sie diese Komponenten:

  - Schutz vor bedrohlichen Dateien.
  - Schutz vor Netzwerkbedrohungen.
  - Schutz vor Web-Bedrohungen.
  - Schutz vor Verschlüsselung.
  - Programmkontrolle.
  - Gerätekontrolle.
  - Überwachung der Systemintegrität.

  Durch die Aktivierung des eBPF-Modus zum Abfangen des Netzwerkdatenverkehrs werden die Telemetriedaten umfassender. Die eBPF-Technologie ist auf Computern mit 64-Bit-Betriebssystemen mit Kernel-Version 4.18 oder höher mit eBPF-Unterstützung verfügbar.

  Wir empfehlen, zu überprüfen, ob Ihr Computer die Komponenten unterstützt, die zum Senden von Telemetriedaten erforderlich sind.

- Fügen Sie den Lizenzschlüssel für EDR Expert (on-premise) zur Anwendung hinzu, wenn Sie eine separate Lizenz zur Nutzung dieser Funktionalität erworben haben.

  Wenn Sie Kaspersky Endpoint Security mit einer Lizenz, die Kaspersky Endpoint Detection and Response Expert (on-premise) umfasst, verwenden, ist keine Aktion erforderlich.

  Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus verwenden, müssen Sie den Lizenzschlüssel zum Aktivieren der zusätzlichen Funktionalität zu den SVMs hinzufügen.

Grundlegende Konfigurationsschritte

1. **Von den Central Node-Servern ausgestellte Zertifikate abrufen und verarbeiten**

   Bei einer Integration mit Kaspersky Anti Targeted Attack Platform stellen die Geräte mit Kaspersky Endpoint Security verschlüsselte HTTPS-Verbindungen zu Servern her, deren Central-Node-Komponente die Integration gewährleistet.

   > Wenn in den allgemeinen Anwendungseinstellungen von Kaspersky Endpoint Security die Verwendung eines Proxyservers konfiguriert ist, wird dieser für die Verbindung mit Servern verwendet, welche die Interaktion mit den Komponenten der Kaspersky Anti Targeted Attack Platform gewährleisten.

   Zertifikate zum Schutz der Verbindungen mit Servern, welche die Interaktion mit den Komponenten der Kaspersky Anti Targeted Attack Platform gewährleisten, werden vom Administrator der Kaspersky Anti Targeted Attack Platform bereitgestellt.

   Um Zertifikate zu verarbeiten, führen Sie die Schritte aus, die im Artikel Konvertieren eines PFX-Zertifikats in das PEM-Format beschrieben sind.

   Sie können ein Serverzertifikat und/oder ein Client-Zertifikat verwenden. Die Auswahl richtet sich nach der Sicherheitsrichtlinie Ihrer Organisation.

2. **Einstellungen für die Integration mit Kaspersky Anti Targeted Attack Platform konfigurieren**

   Diese können Sie wie folgt konfigurieren:

   - Über die Web Console (EDR (KATA) und NDR (KATA) in der Konsole von Kaspersky Security Center und/oder in der OSMP-Konsole).
   - Über die Kaspersky Security Center Verwaltungskonsole (EDR (KATA) und NDR (KATA)).
   - Über die Befehlszeile (EDR (KATA) und NDR (KATA)).

3. **Stellen Sie sicher, dass die Verbindung mit Kaspersky Anti Targeted Attack Platform erfolgreich hergestellt wurde.**

   Überprüfen Sie den Status der Komponenten von Kaspersky Anti Targeted Attack Platform mit einer beliebigen geeigneten Methode.

4. **Bei Bedarf zusätzliche Einstellungen verwalten**

   - Wenn SELinux in Ihrem Betriebssystem im Enforcing-Modus konfiguriert ist, müssen Sie SELinux zusätzlich konfigurieren, um Reaktionsaktionen auszuführen.
   - Machen Sie sich mit den Einschränkungen der Netzwerkisolation vertraut.

So konfigurieren Sie die EDR (KATA)-Integration

In der Web Console können Sie die Komponente Kaspersky Endpoint Detection and Response (KATA) aktivieren oder deaktivieren und die Integration des Programms Kaspersky Endpoint Security mit dieser Komponente konfigurieren.

So konfigurieren Sie die Integration mit Kaspersky Endpoint Detection and Response (KATA) in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

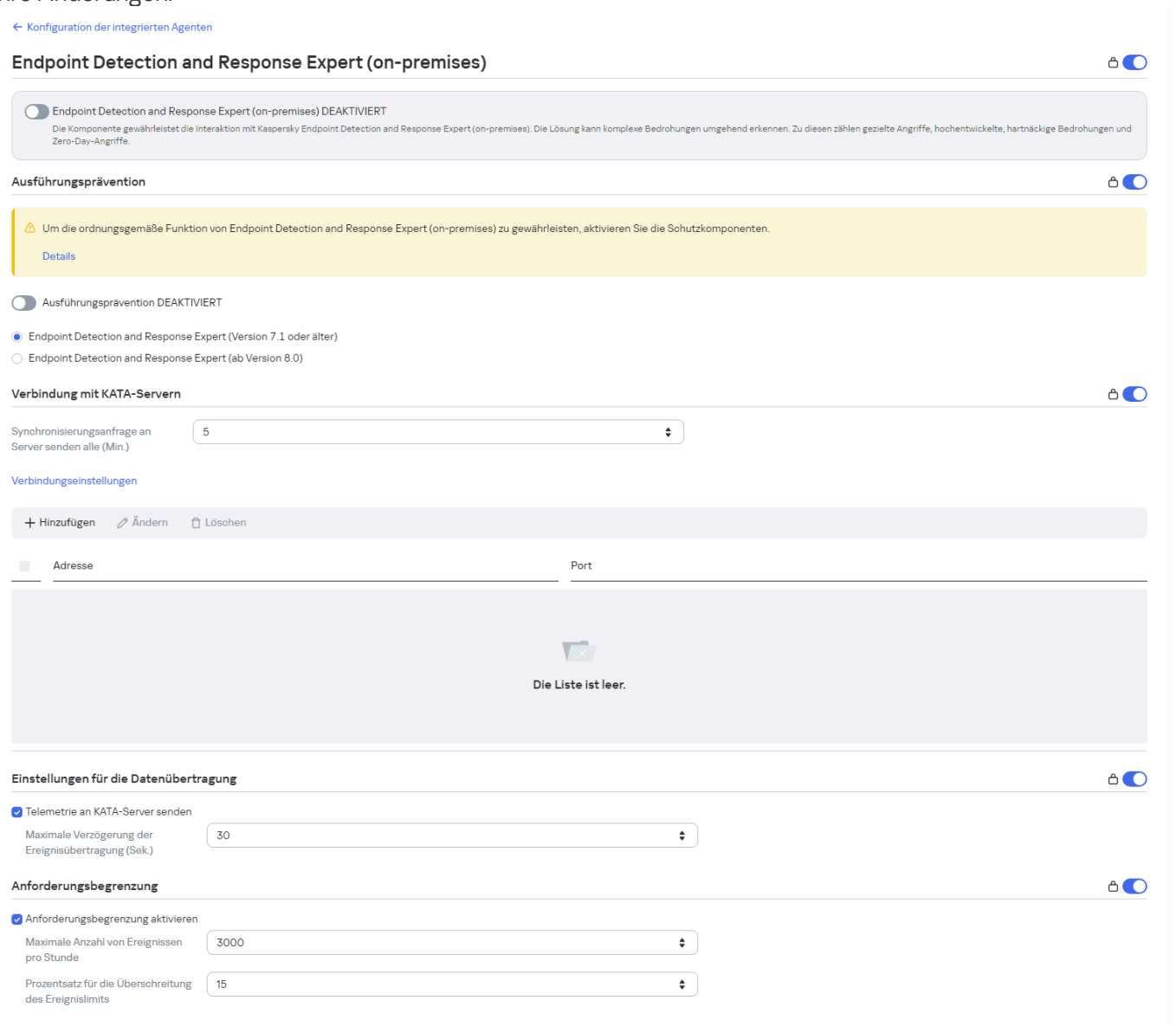
   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie im geöffneten Fenster mit den Richtlinieneigenschaften die Registerkarte **Programmeinstellungen** aus.
5. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response Expert (On-Premises)**.
6. Im rechten Bildschirmbereich:
   a. Wählen Sie die Option **Endpoint Detection and Response Expert Version 7.1 oder früher** aus.
   b. Wählen Sie im Abschnitt **Verbindung mit Servern zur Erfassung von Telemetriedaten** einen Server zur Erfassung von Telemetriedaten aus, indem Sie in der Symbolleiste auf die Schaltfläche **Hinzufügen** klicken, und klicken Sie anschließend auf **Server auswählen**.
   c. Wählen Sie im Abschnitt **Verbindung mit Reaktionsservern** einen Reaktionsserver aus, indem Sie in der Symbolleiste auf die Schaltfläche **Hinzufügen** klicken, und klicken Sie anschließend auf **Server auswählen**.
   d. Klicken Sie in den Abschnitten **Verbindung mit Servern zur Erfassung von Telemetriedaten** und **Verbindung mit Servern zur Reaktion auf Bedrohungen** auf den Link **Verbindungseinstellungen** und nehmen Sie anschließend im angezeigten Bereich folgende Einstellungen vor:
      1. Fügen Sie ein Serverzertifikat hinzu, indem Sie auf die Schaltfläche **Hochladen** klicken.
      2. Wenn Sie zusätzlichen Schutz benötigen, erstellen Sie einen Crypto-Container.

         Gehen Sie dazu im Abschnitt **Zusätzlicher Verbindungsschutz** wie folgt vor:

         - Aktivieren Sie das Kontrollkästchen **Zwei-Wege-Authentifizierung verwenden**.
         - Klicken Sie auf die Schaltfläche **Hochladen** und fügen Sie das Client-Zertifikat hinzu, das Sie in Schritt 1 des Hauptszenarios erhalten haben.
         - Geben Sie im entsprechenden Feld ein Kennwort für den Crypto-Container ein.

         Das Feld **Kennwort für Crypto-Container** ist erforderlich. Sie können die Einstellungen nicht speichern, ohne ein Kennwort für das Client-Zertifikat (Crypto-Container) einzugeben.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Endpoint Detection and Response Expert (On-Premises)

So konfigurieren Sie die Integration mit Kaspersky Endpoint Detection and Response (KATA) über die Befehlszeile

1. Um einen Modus der EDR (KATA)-Integration auszuwählen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 24 Mode=EDRKATA
```

2. Um einen Central Node-Server hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 24 Endpoints.item_001.Address=<central node server address>
Endpoints.item_001.Port=<central node server port>
```

3. Um ein Zertifikat für den Response-Server hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

4. Um die Integrationseinstellungen zu konfigurieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 24 [<setting name>=<setting value>]
```

Die Einstellungen und ihre möglichen Werte sind in der folgenden Tabelle aufgeführt.

5. Um ein Client-Zertifikat für die Verbindung mit dem Response-Server hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

6. Um die Integration mit EDR (KATA) zu aktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --start-task 24
```

Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA)

Parameter	Description	Wert
`Mode`	Modus der Integration. Bei der Integration in Kaspersky Endpoint Detection and Response Expert (on-premise) interagiert das Programm Kaspersky Endpoint Security mit Servern auf der OSMP-Plattform. Bei einer Integration mit Kaspersky Endpoint Detection and Response (KATA) kommuniziert Kaspersky Endpoint Security mit Servern auf der Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (Standardwert) – Integration im Modus EDR (KATA). Erlaubt die Integration mit Kaspersky Endpoint Detection and Response (KATA). Dies ist eine Komponente von Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` ist der Integrationsmodus EDR Expert (on-premise). Aktiviert die Integration in Kaspersky Endpoint Detection and Response Expert (on-premise)
`UseClientPinnedCertificate`	Aktivieren und Deaktivieren der Zwei-Wege-Authentifizierung, um die Verbindung zum KATA-Server zusätzlich abzusichern. Wenn die Zwei-Wege-Authentifizierung aufseiten des KATA-Servers aktiviert ist, müssen Sie vor dem Starten der Aufgabe die Zwei-Wege-Authentifizierung in den Einstellungen der Aufgabe *Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)* aktivieren und das Client-Zertifikat hinzufügen.	`Yes` – Zwei-Wege-Authentifizierung verwenden, um die Verbindung zum KATA-Server zusätzlich abzusichern. `No` (Standardwert) – Zwei-Wege-Authentifizierung nicht verwenden.
`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`.
`EnableTelemetry`	Senden von Ereignisdaten (Telemetriedaten) an KATA.	`Yes` (Standardwert) – Telemetriedaten an den KATA-Server senden `No` – keine Telemetriedaten senden
Der Abschnitt **[Endpoints.item_#]** enthält die Adresse und den Port des KATA-Servers. Sie können mehrere Server hinzufügen.		
`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 Server nicht unterbrochen wird, wenn die Anwendung 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`.
Der Abschnitt **[EventTransferSettings]** enthält Parameter für die Übertragung von Daten an den KATA-Server.		

Parameter	Description	Wert
`MaximumDataTransferTime`	Maximale Verzögerung beim Senden von Ereignissen an den KATA-Server in Sekunden.	Der Standardwert ist: `30`.
`UseRequestCountLimits`	Begrenzung der Anzahl der an den KATA-Server gesendeten Ereignisse aktivieren und deaktivieren.	`Yes` (Standardwert) – die Anzahl der gesendeten Ereignisse wird begrenzt `No` – die Anzahl der gesendeten Ereignisse wird nicht begrenzt
`MaximumNumberOfEventsInHour`	Maximale Anzahl an Ereignissen pro Stunde	Der Standardwert ist: `3000`.
`MaximumNumberOfEventsInPackage`	Die maximale Anzahl von Ereignissen in einem Paket.	Der Standardwert ist: `1024`.
`EventLimitExceededPercentage`	Prozentuale Überschreitung der Beschränkung der Ereignisanzahl: 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`.

Wenn Sie die Web Console oder die Befehlszeile verwenden, müssen Sie für die Integration mit Kaspersky Endpoint Detection and Response (KATA) in den Einstellungen der Komponente EDR Expert (on-premise) den Integrationsmodus *EDR (KATA)* auswählen:

- Wenn Sie die Web Console verwenden, wählen Sie in den Richtlinieneinstellungen die Option **Endpoint Detection and Response Expert (Version 7.1 oder älter)** aus. Um die Integration mit Kaspersky Endpoint Detection and Response (KATA) auf einem Gerät zu konfigurieren, müssen Sie in der Web Console die „Schlösser“ verwalten – entweder für Version 8.0 und höher oder für Version 7.1 und früher.

- Wenn Sie die Befehlszeile verwenden, geben Sie in den Aufgabeneinstellungen den Parameter `Mode=EDRKATA` an.

So konfigurieren Sie die NDR (KATA)-Integration

In der Web Console können Sie die Komponente Kaspersky Network Detection and Response (KATA) aktivieren oder deaktivieren und die Integration des Programms Kaspersky Endpoint Security mit dieser Komponente konfigurieren.

So konfigurieren Sie die Integration mit Kaspersky Network Detection and Response (KATA) in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Network Detection and Response (KATA)**.
5. Aktivieren Sie den Schalter **Network Detection and Response (KATA)**.
6. Klicken Sie auf die Schaltfläche **Verbindungseinstellungen**.

7. Konfigurieren Sie die Serververbindung:

   - **Timeout (Sek.)**. Maximale Zeitüberschreitung für die Antwort von Central Node. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Central Node-Server zu verbinden.

   - **Serverzertifikat**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Central Node-Server. Ein TLS-Zertifikat können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform).

   - **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Aufbau einer sicheren Verbindung zwischen Kaspersky Endpoint Security und dem Central Node-Server. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Central Node-Servers aktivieren, dann einen Krypto-Container anfordern und ein Kennwort festlegen, um den Krypto-Container zu schützen. Ein *Krypto-Container* ist ein PFX-Archiv mit einem Zertifikat und einem privaten Schlüssel. Einen Krypto-Container können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform). Nachdem Sie die Central Node-Einstellungen konfiguriert haben, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen von Kaspersky Endpoint Security aktivieren und einen kennwortgeschützten Krypto-Container laden.

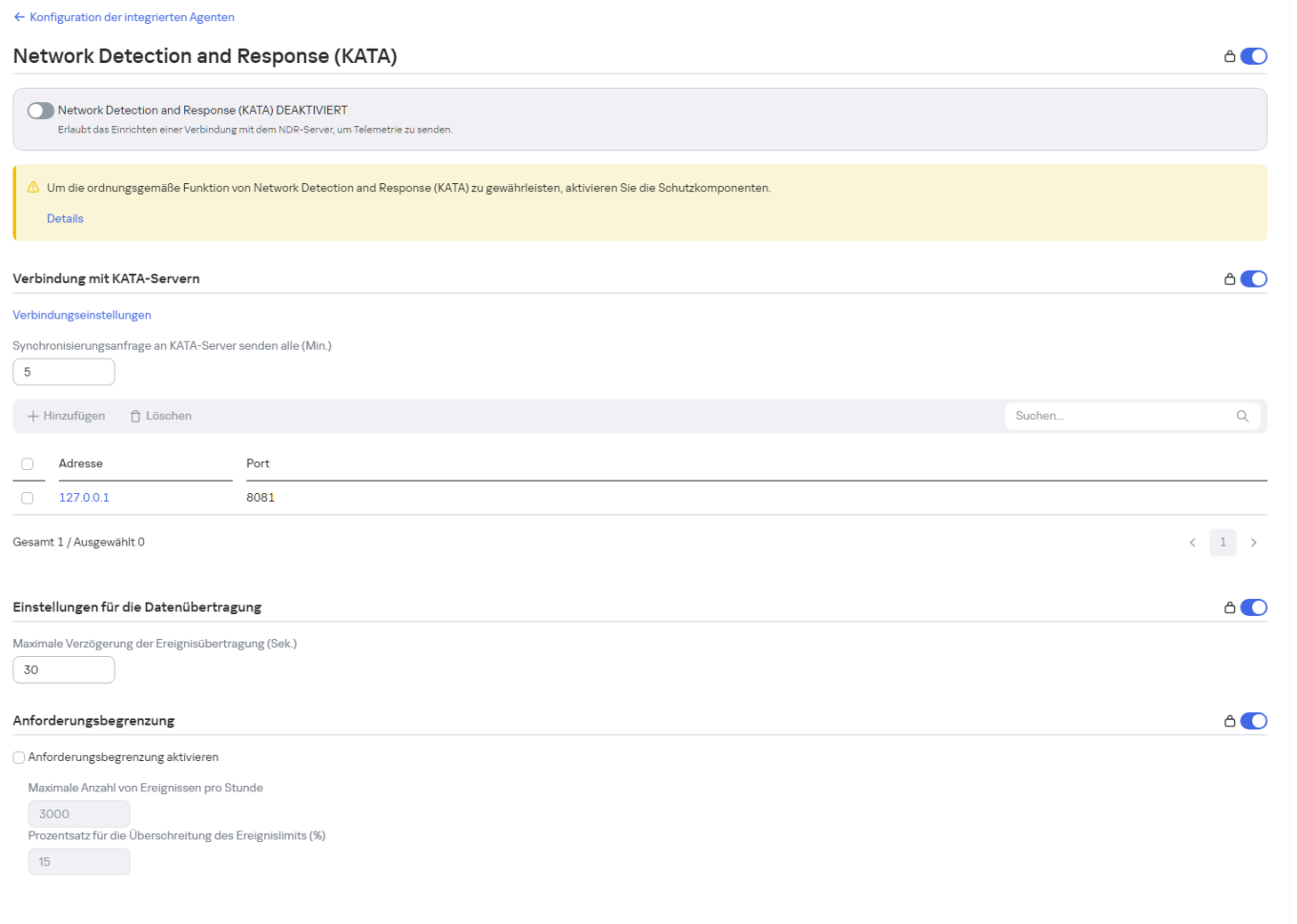
     Der Krypto-Container muss kennwortgeschützt sein. Ein Krypto-Container mit einem leeren Passwort kann nicht hinzugefügt werden.

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

9. Fügen Sie Central Node-Server hinzu. Geben Sie dazu die Serveradresse (IPv4, IPv6) und den Port für die Serververbindung an.

10. Sie können mehrere Serveradressen für Central Node hinzufügen. Kaspersky Endpoint Security versucht, sich über die erste IP-Adresse mit dem Server zu verbinden. Wenn keine Verbindung hergestellt werden kann, versucht Kaspersky Endpoint Security eine Verbindung mit der zweiten IP-Adresse in der Liste und so weiter.

11. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Network Detection and Response (KATA)

So konfigurieren Sie die Integration mit Kaspersky Network Detection and Response (KATA) über die Befehlszeile

1. Um einen Central Node-Server hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 31 Endpoints.item_001.Address=<central node server address>
Endpoints.item_001.Port=<central node server port>
```

2. Um ein Zertifikat für den Response-Server hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

3. Um die Integrationseinstellungen zu konfigurieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 31 [<setting name>=<setting value>]
```

Die Einstellungen und ihre möglichen Werte sind in der folgenden Tabelle aufgeführt.

4. Um ein Client-Zertifikat für die Verbindung mit dem Response-Server hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

5. Um die Integration mit NDR (KATA) zu aktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --start-task 31
```

Einstellungen der Aufgabe zur Integration mit Kaspersky Network Detection and Response (KATA)

Einstellung	Description	Wert
`UseClientPinnedCertificate`	Aktivieren und Deaktivieren der Zwei-Wege-Authentifizierung, um die Verbindung zum NDR-Server zusätzlich abzusichern. Wenn die Überprüfung des Client-Zertifikats auf der Seite des NDR-Servers aktiviert ist, müssen Sie die Verwendung des Client-Zertifikats aktivieren und das Client-Zertifikat hinzufügen, bevor Sie die Aufgabe *Integration mit Kaspersky Network Detection and Response (KATA)* ausführen.	`Yes` – Zwei-Wege-Authentifizierung verwenden, um die Verbindung zum NDR-Server zusätzlich abzusichern. `No` (Standardwert) – Zwei-Wege-Authentifizierung nicht verwenden.
`SynchronizationPeriod`	Häufigkeit des Sendens von Synchronisierungsanfragen an den NDR-Server in Minuten.	Der Standardwert ist: `5`.
`ConnectionTimeout`	Die maximale Wartezeit auf eine Verbindung mit dem NDR-Server in Sekunden.	Der Standardwert ist: `10`.
`RequestTimeout`	Die maximale Wartezeit auf eine Antwort vom NDR-Server in Sekunden.	Der Standardwert ist: `10`.
Der Abschnitt **[Endpoints.item_#]** enthält die Adresse und den Port des NDR-Servers.		
`Address`	Adresse des NDR-Servers. Sie können die IP-Adresse (IPv4 oder IPv6) oder den vollqualifizierten Domänennamen (FQDN) des Servers angeben.	Der Standardwert ist: `127.0.0.1`.
`Port`	Port für die Verbindung zum NDR-Server.	Der Standardwert ist: `8081`.
Der Abschnitt **[EventTransferSettings]** enthält Parameter für die Übertragung von Ereignissen an den NDR-Server.		
`MaximumDataTransferTime`	Maximale Verzögerung beim Senden von Ereignissen an den NDR-Server in Sekunden.	Der Standardwert ist: `30`.
`MaximumNumberOfEventsInPackage`	Die maximale Anzahl von Ereignissen in einem Paket.	Der Standardwert ist: `1024`.
`UseRequestCountLimits`	Begrenzung der Anzahl der an den NDR-Server gesendeten Ereignisse aktivieren und deaktivieren.	`Yes` (Standardwert) – die Anzahl der gesendeten Ereignisse wird begrenzt `No` – die Anzahl der gesendeten Ereignisse wird nicht begrenzt
`MaximumNumberOfEventsInHour`	Maximale Anzahl an Ereignissen pro 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`.
`PingPeriod`	Häufigkeit der Abfrage von NDR-Servern in Sekunden.	Der Standardwert ist: `450`.

So überprüfen Sie, ob die KATA-Integration ausgeführt wird

Sie können die Komponenten von Kaspersky Anti Targeted Attack Platform auf folgende Weise testen:

- Über die Befehlszeile mit folgendem Befehl:

```
kesl-control --app-info
```

Für die Integration mit den Komponenten EDR (on-premises) und NDR (KATA) wird der Status **Verfügbar und wird ausgeführt** angezeigt.

- In der Web Console:
  - In der Konsole von Kaspersky Security Center verwenden Sie den *Bericht über den Status der Programmkomponenten*. Weitere Informationen zum Umgang mit Berichten finden Sie in der Hilfe zu Kaspersky Security Center.
  - In der OSMP-Konsole:
    - Mithilfe des *Berichts über den Status der Programmkomponenten*.
    - Wechseln Sie zum Abschnitt **Asset-Management** → **Assets** und wählen Sie die Registerkarte **Analyse und Reaktion** aus.

      Das Gerät wird in der Liste mit dem Telemetriedatenstatus **Normale Aktivität** angezeigt.
    - Wechseln Sie zum Abschnitt **Bedrohungssuche**.

      Telemetriedatenereignisse vom Gerät werden in der Liste der Ereignisse angezeigt.
- In Kaspersky Anti Targeted Attack Platform:

  Wechseln Sie zum Abschnitt **Assets** → **Geräte**. Die Geräte werden in der Tabelle angezeigt. Bei Bedarf können Sie die Tabelle nach **EPP-Anwendung**, **EPP-Verbindung** und **Zuletzt mit EPP verbunden** filtern.

  Durch Klicken auf den Namen eines Geräts wird ein Bereich geöffnet. Im Abschnitt **Endpoint Agent** ist der Verbindungsstatus **Aktiv**.

Sandbox

Die Sandbox-Technologie ermöglicht die Analyse und Untersuchung von Objekten auf speziellen Servern mit installierten virtuellen Images von Betriebssystemen, um schädliche Aktivitäten und Anzeichen gezielter Angriffe auf die IT-Infrastruktur der Organisation zu erkennen.

Das Programm Kaspersky Endpoint Security kann über die Open Single Management Platform (OSMP) oder die Kaspersky Anti Targeted Attack Platform mit Sandbox interagieren.

Die Komponente ist für Geräte mit Elbrus-CPU nicht verfügbar.

So konfigurieren Sie die Integration mit Sandbox

Bevor Sie mit der Konfiguration der Integration mit Sandbox beginnen:

- Lassen Sie eingehende und ausgehende Verbindungen wie folgt zu:
  - Eingehend (Verwaltungsschnittstelle):
    - TCP 22
    - TCP 443
    - TCP 8443

- Ausgehend (Verwaltungsschnittstelle):
  - TCP 80 oder TCP 443
- Ausgehend und entsprechend eingehend (Schnittstelle für den Zugriff auf verarbeitete Objekte):

  Beliebiger Port.

- Installieren Sie die grafische Benutzeroberfläche (das Paket kesl-gui), wenn Sie Dateien manuell über das Kontextmenü einer Datei oder eines Verzeichnisses an die Sandbox senden möchten.

Grundlegende Konfigurationsschritte

1. **Erstellen Sie auf der Plattform eine Verbindungsanfrage für den Sandbox-Server und bestätigen Sie anschließend die Verbindung in der Sandbox-Verwaltungskonsole**

   Ausführliche Informationen finden Sie in der Hilfe zu den jeweiligen Lösungen:

   - Kaspersky Anti Targeted Attack Platform
   - Open Single Management Platform

   Speichern Sie die IP-Adresse des Sandbox-Servers auf eine beliebige geeignete Weise. Sie benötigen sie für die spätere Konfiguration der Integration.

2. **Rufen Sie die Zertifikate ab, die vom OSMP-Server oder vom Server Zentralknoten ausgestellt wurden, und verarbeiten Sie sie**

   Während der Integration mit Sandbox stellt ein Gerät mit Kaspersky Endpoint Security per HTTPS-Protokoll eine sichere Verbindung mit den Servern her, welche die Kommunikation gewährleisten.

   > Wenn in den allgemeinen Einstellungen der Anwendung Kaspersky Endpoint Security die Verwendung eines Proxyservers konfiguriert ist, wird für die Verbindung mit Servern, die die Interaktion mit Sandbox abwickeln, ein Proxyserver verwendet.

   Die Zertifikate zur Absicherung der Verbindungen mit den Servern, welche die Interaktion mit Sandbox gewährleisten, werden vom Administrator von der OSMP-Plattform oder von Kaspersky Anti Targeted Attack Platform bereitgestellt.

   Um Zertifikate zu verarbeiten, führen Sie die Schritte aus, die im Artikel Konvertieren eines PFX-Zertifikats in das PEM-Format beschrieben sind.

   Sie können ein Serverzertifikat und/oder ein Client-Zertifikat verwenden. Die Auswahl richtet sich nach der Sicherheitsrichtlinie Ihrer Organisation.

3. **Einstellungen der Integration mit Sandbox verwalten**

   Um Dateien zur Untersuchung zu senden, müssen Sie die Integration in KATA Sandbox aktivieren und einen Central Node-Server hinzufügen, der innerhalb der Lösung bereitgestellt wird.

   So konfigurieren Sie die Integration mit Sandbox in der Web Console

   1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
   2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

      Das Eigenschaftenfenster der Richtlinie wird geöffnet.
   3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Konfiguration der integrierten Agenten → Sandbox**.

5. Wählen Sie in der Dropdown-Liste **Typ der Datei-Übermittlung für die Untersuchung** die erforderliche Methode aus:

   - **Manuell**. In diesem Modus können Sie Objekte manuell mithilfe eines Befehls oder über das Kontextmenü **Mit der Sandbox untersuchen** zur Untersuchung an die Sandbox senden.

     Wir empfehlen, diesen Typ auszuwählen, wenn Ihre Sandbox-Version älter als 8.0 ist.

   - **Automatisch**. Die Anwendung versendet die Objekte automatisch zur Untersuchung. Das manuelle Versenden von Objekten zur Untersuchung an die Sandbox ist nicht möglich.

   - **Kombiniert**. Die Anwendung versendet die Objekte automatisch zur Untersuchung. Zusätzlich können Sie Objekte per Befehl manuell oder über die grafische Oberfläche zur Untersuchung an die Sandbox versenden.

6. Im Abschnitt **Verbindung mit Sandbox-Servern**:

   - Fügen Sie den Integrationsserver hinzu, indem Sie in der Symbolleiste auf die Schaltfläche **Hinzufügen** klicken.

     Sie können als Adresse die IP-Adresse der KATA-/OSMP-Plattform oder deren FQDN angeben.

     Wenn der Sandbox-Server mit OSMP verbunden ist, können Sie nur den FQDN des Agent-Servers angeben.

   - Fügen Sie das Serverzertifikat von Kaspersky Anti Targeted Attack Platform oder OSMP hinzu, das Sie in Schritt 2 des Hauptszenarios erhalten haben.

     Klicken Sie dazu auf den Link **Einstellungen der Serververbindung**, und klicken Sie anschließend im angezeigten Bereich im Abschnitt **TLS-Serverzertifikat** auf die Schaltfläche **Hochladen**.

   - Wenn Sie zusätzlichen Schutz benötigen, erstellen Sie einen Crypto-Container.

     Führen Sie dazu im Abschnitt **Erhöhte Verbindungssicherheit** folgende Schritte aus:

     - Aktivieren Sie das Kontrollkästchen **Zwei-Wege-Authentifizierung verwenden**.
     - Klicken Sie auf die Schaltfläche **Hochladen** und fügen Sie ein Client-Zertifikat hinzu.
     - Geben Sie im entsprechenden Feld ein Kennwort für den Crypto-Container ein.

     Das Feld **Kennwort des Krypto-Containers** ist ein Pflichtfeld. Sie können die Einstellungen nicht speichern, ohne ein Kennwort für das Client-Zertifikat (Crypto-Container) einzugeben.

7. Wählen Sie die entsprechende Aktion im Block **Aktion beim Fund einer Bedrohung**:

   - **Kopie in die Quarantäne verschieben, Objekt löschen**. Wenn diese Option ausgewählt ist, löscht Kaspersky Endpoint Security das auf dem Computer gefundene schädliche Objekt. Bevor das Objekt gelöscht wird, erstellt Kaspersky Endpoint Security ein Backup davon für den Fall, dass Sie das Objekt später wiederherstellen möchten. Kaspersky Endpoint Security verschiebt die Backup-Kopie in die Quarantäne.

   - **Untersuchung wichtiger Bereiche ausführen**. Wenn diese Option ausgewählt ist, führt Kaspersky Endpoint Security die *Untersuchung wichtiger Bereiche* aus. Standardmäßig überprüft Kaspersky Endpoint Security den Kernel-Speicher, die gestarteten Prozesse und die Bootsektoren.

   - **IOC-Untersuchungsaufgabe erstellen**. Wenn diese Option ausgewählt ist, erstellt Kaspersky Endpoint Security automatisch die *IOC-Untersuchung (eigenständige IOC-Untersuchungsaufgabe)*. Für diese Aufgabe können Sie den Ausführungsmodus, den Untersuchungsbereich und die Aktion bei einer IOC-Erkennung anpassen (*Kopie in die Quarantäne verschieben, Objekt löschen* oder *Untersuchung wichtiger Bereiche ausführen*). Um andere Einstellungen der Aufgabe *IOC-Untersuchung* zu ändern, gehen Sie zu den Aufgabeneinstellungen.

8. Konfigurieren Sie, sofern erforderlich, die Einstellungen der Aufgabe *IOC-Untersuchung* im Block **IOC-Untersuchungsbereich**.

   - **Bereiche mit kritischen Dateien**. Wenn diese Option ausgewählt ist, sucht Kaspersky Endpoint Security nur in Benutzer- und Systemverzeichnissen nach IOCs.

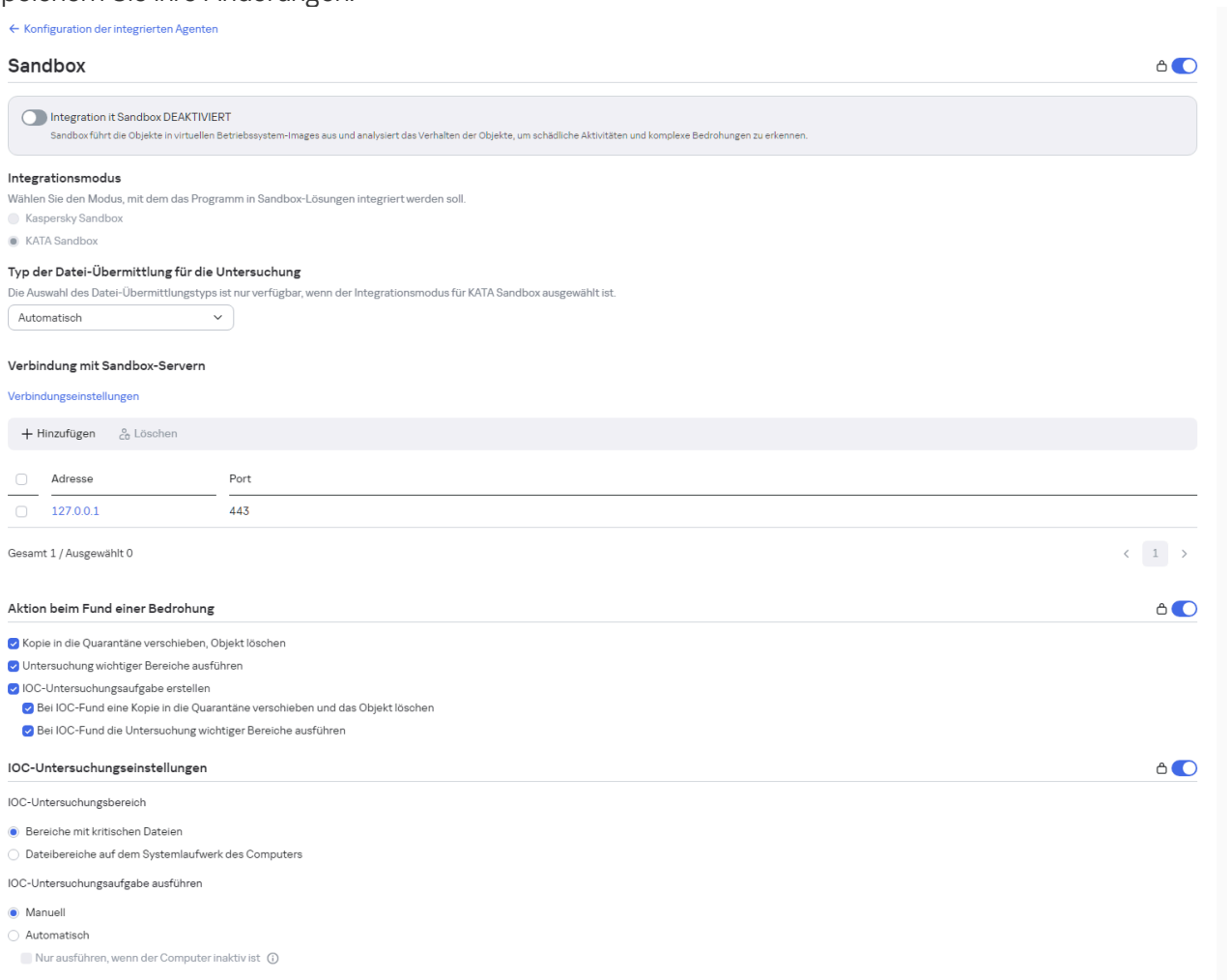
   - **Dateibereiche auf dem Systemlaufwerk des Computers**. Wenn diese Option ausgewählt ist, untersucht Kaspersky Endpoint Security alle Dateien im Root-Dateisystem auf IOCs.

9. Konfigurieren Sie, sofern erforderlich, die Einstellungen der Aufgabe *IOC-Untersuchung* im Block **IOC-Untersuchungsaufgabe ausführen**.

   - **Manuell**. In diesem Ausführungsmodus können Sie die Aufgabe *IOC-Untersuchung* zu einem geeigneten Zeitpunkt manuell starten.

   - **Automatisch**. Ausführungsmodus, in dem Kaspersky Endpoint Security die Aufgabe *IOC-Untersuchung* automatisch ausführt, nachdem eine Bedrohung erkannt wurde.

10. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Sandbox

So konfigurieren Sie die Integration mit Sandbox über die Befehlszeile

1. Um ein Serverzertifikat hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

2. Um einen Zentralknoten oder einen OSMP-Server hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 29 Servers.item_0000.Address=<server> Servers.item_0000.Port=<port>
```

3. Um die Integrationseinstellungen zu konfigurieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 29 [<setting name>=<setting value>]
```

Die Einstellungen und ihre möglichen Werte sind in der folgenden Tabelle aufgeführt.

4. Um ein Client-Zertifikat hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

5. Um die Integration mit Sandbox zu aktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --start-task 29
```

Einstellungen der Aufgabe zur Integration mit Sandbox

Parameter	Description	Wert
`UseClientCertificate`	Aktivieren und Deaktivieren der Zwei-Wege-Authentifizierung, um die Verbindung zum Sandbox-Server zusätzlich abzusichern. Wenn die Überprüfung des Client-Zertifikats auf der Seite des Sandbox-Servers aktiviert ist, müssen Sie die Verwendung des Client-Zertifikats aktivieren und das Client-Zertifikat hinzufügen, bevor Sie die Aufgabe *Integration mit Sandbox* ausführen.	`Yes` – Zwei-Wege-Authentifizierung verwenden, um die Verbindung zum Sandbox-Server zusätzlich abzusichern. `No` (Standardwert) – Zwei-Wege-Authentifizierung nicht verwenden.
`ConnectionTimeout`	Die maximale Wartezeit auf eine Verbindung mit dem Server in Sekunden.	Der Standardwert ist: `10`.
`RequestTimeout`	Die maximale Wartezeit auf eine Antwort vom Server in Sekunden.	Der Standardwert ist: `10`.
`SendingMode`	Modus zum Senden der Datei zur Untersuchung an die Sandbox	`AutoOnly` (Standardwert) – Dateien werden beim Zugriff automatisch zur Untersuchung gesendet. `Manual` – Dateien werden manuell zur Untersuchung gesendet. `AutoAndManual` – Dateien werden sowohl automatisch als auch manuell zur Untersuchung gesendet.
`QuarantineFile`	Datei nach Erkennung einer Bedrohung in die Quarantäne verschieben.	`Yes` (Standardwert) – Bei Erkennung einer Bedrohung wird die ursprüngliche Datei gelöscht und eine Kopie der Datei in die Quarantäne verschoben. `No` – Bei Erkennung einer Bedrohung wird die Datei nicht in die Quarantäne verschoben.
`ScanCriticalAreas`	Führt die Untersuchung wichtiger Bereiche bei Erkennung einer Bedrohung aus.	`Yes` (Standardwert) – Bei Erkennung einer Bedrohung wird die Untersuchung wichtiger Bereiche gestartet. `No` – Bei Erkennung einer Bedrohung wird die Untersuchung wichtiger Bereiche nicht gestartet.
`CreateIocScanTask`	Erstellt bei Erkennung einer Bedrohung eine Aufgabe zur IOC-Untersuchung.	`Yes` (Standardwert) – Bei Erkennung einer Bedrohung wird eine Aufgabe zur IOC-Untersuchung erstellt. `No` – Bei Erkennung einer Bedrohung wird keine Aufgabe zur IOC-Untersuchung erstellt.
`QuarantineFileOnIocDetected`	Objekt nach Erkennung eines Kompromittierungsindikators in die Quarantäne verschieben.	`Yes` (Standardwert) – Bei Erkennung eines Kompromittierungsindikators wird das ursprüngliche Objekt gelöscht und eine Kopie des Objekts in die Quarantäne verschoben. `No` – Bei Erkennung eines Kompromittierungsindikators wird das Objekt nicht in die Quarantäne verschoben.
`ScanCriticalAreasOnIocDetected`	Führt die Untersuchung wichtiger Bereiche bei Erkennung eines Kompromittierungsindikators aus.	`Yes` (Standardwert) – Bei Erkennung eines Kompromittierungsindikators wird die Untersuchung wichtiger Bereiche gestartet. `No` – Bei Erkennung eines Kompromittierungsindikators wird die Untersuchung wichtiger Bereiche nicht gestartet.

Parameter	Description	Wert
`Drives`	Bereiche, die auf Kompromittierungsindikatoren untersucht werden.	`Critical` (Standardwert) – Untersucht Dateien in benutzerdefinierten Verzeichnissen und Systemverzeichnissen. `System` – Untersucht alle Dateien innerhalb des Stamm-Dateisystems.
`ScheduleMode`	Ausführungsmodus der Aufgabe zur IOC-Untersuchung.	`Manually` (Standardwert) – IOC-Untersuchung manuell ausführen. `AfterTreatDetected` – IOC-Untersuchung nach Erkennung einer Bedrohung ausführen.
Der Abschnitt **[Servers.item_#]** enthält die Parameter des Sandbox-Servers.		
`Address`	Adresse des Servers. Sie können die IP-Adresse (IPv4 oder IPv6) oder den vollqualifizierten Domänennamen (FQDN) des Servers angeben.	Der Standardwert ist: `127.0.0.1`.
`Port`	Port für die Verbindung zum Server.	Der Standardwert ist: `443`.
Der Abschnitt **[SandboxTransferSettings]** enthält Parameter für die Übertragung von Dateien zur Untersuchung in Sandbox.		
`SandboxQueue`	Die maximale Größe des Verzeichnisses zum Speichern der Warteschlange für Untersuchungsanfragen in Megabyte.	Der Standardwert ist: `1024`.

4. **Überprüfen Sie, ob die Verbindung zur Sandbox erfolgreich hergestellt wurde**

   Überprüfen Sie den Status von Sandbox auf beliebige geeignete Weise.

So überprüfen Sie, ob die Integration mit Sandbox ausgeführt wird

Sie können die Sandbox-Komponente auf folgende Arten testen:

- Über die Befehlszeile mit folgendem Befehl:

  ```
  kesl-control --app-info
  ```

  Die Integration mit Sandbox wird mit dem Status **Verfügbar und wird ausgeführt** angezeigt.

- In der Web Console:

  - Berichte in der Kaspersky Security Center-Konsole:

    Mithilfe des *Berichts über den Status der Programmkomponenten*. Weitere Informationen zum Umgang mit Berichten finden Sie in der Hilfe zu Kaspersky Security Center.

  - In der OSMP-Konsole:

    - Mithilfe des *Berichts über den Status der Programmkomponenten*.
    - Wechseln Sie zum Abschnitt **Bedrohungssuche**.

      Ereignisse zu erfolgreichen Sandbox-Verbindungen werden in der Ereignisliste angezeigt.

- In Kaspersky Anti Targeted Attack Platform:

  Wechseln Sie zum Abschnitt **Assets** → **Geräte**. Die Geräte werden in der Tabelle angezeigt. Bei Bedarf können Sie die Tabelle nach **EPP-Anwendung**, **EPP-Verbindung** und **Zuletzt mit EPP verbunden** filtern.

Durch Klicken auf den Namen eines Geräts wird ein Bereich geöffnet. Im Abschnitt Endpoint Agent lautet der Verbindungsstatus **Aktiv**.

So senden Sie eine Datei manuell an Sandbox

Kaspersky Endpoint Security ermöglicht es Benutzern, Dateien oder Verzeichnisse über das Kontextmenü manuell zur Untersuchung in die Sandbox zu senden.

Um Dateien zur Untersuchung in der Sandbox zu senden, müssen die folgenden Bedingungen erfüllt sein:

- Die grafische Benutzeroberfläche von Kaspersky Endpoint Security muss installiert sein.
- Kaspersky Endpoint Security muss mit Sandbox integriert sein.
- Der Modus zum Senden von Dateien zur Untersuchung muss auf **Manuell** oder **Kombiniert** festgelegt sein.

So senden Sie eine Datei oder ein Verzeichnis zur Untersuchung an die Sandbox:

1. Öffnen Sie das Kontextmenü der zu untersuchenden Datei bzw. des zu untersuchenden Verzeichnisses.
2. Wählen Sie **Kaspersky Endpoint Security 12.5 für Linux** als Anwendung zum Öffnen der Datei oder des Verzeichnisses aus.

   Die Namen der Elemente im Kontextmenü kann je nach Desktop-Umgebung variieren.

3. Wählen Sie anschließend im Kontextmenü **Mit der Sandbox untersuchen** aus.

Kaspersky Managed Detection and Response

Kaspersky Endpoint Security enthält einen integrierten Agenten für die Integration mit der Lösung Kaspersky Managed Detection and Response. Die Lösung *Kaspersky Managed Detection and Response (MDR)* erkennt und analysiert automatisch Sicherheitsvorfälle in Ihrer Infrastruktur. Zu diesem Zweck verwendet MDR von Endpunkten bereitgestellte Telemetriedaten sowie maschinelles Lernen. MDR sendet Vorfalldaten an die Kaspersky-Experten. Die Experten können den Vorfall dann bearbeiten und beispielsweise einen neuen Eintrag zu den Antiviren-Datenbanken hinzufügen. Alternativ können die Experten Tipps zum Umgang mit dem Vorfall geben und beispielsweise vorschlagen, bestimmte Computer vom Netzwerk zu isolieren. Ausführliche Informationen zur Funktionsweise der Lösung finden Sie in der Hilfe zu „Kaspersky Managed Detection and Response“.

Die Integration erfolgt durch Kaspersky Endpoint Security – Managed Detection and Response (im Weiteren auch "MDR"). Die Komponente muss auf eine der im Integrationsszenario beschriebenen Weisen aktiviert werden.

Die Komponente ist für Geräte mit Elbrus-CPU nicht verfügbar.

Konfigurationen von Kaspersky Endpoint Security für die Integration in MDR

Die folgenden Konfigurationen können für die Arbeit mit MDR verwendet werden:

- **[KES+built-in agent]**. In dieser Konfiguration dient Kaspersky Endpoint Security sowohl als Programm, das die Sicherheit des Computers gewährleistet, als auch als Programm für die Interaktion mit MDR.
- **[third-party EPP+EDR Agent]**. In dieser Konfiguration wird die Sicherheit der IT-Infrastruktur durch die Endpoint Protection Platform (EPP) eines Drittanbieters bereitgestellt. In der Konfiguration Endpoint Detection and Response Agent (EDR Agent) wird die Interaktion mit MDR durch Kaspersky Endpoint Security gewährleistet. In dieser Konfiguration ist EDR Agent mit EPP-Anwendungen von Drittanbietern kompatibel.

Empfehlungen zum Erstellen eines Referenzabbilds für die korrekte Integration mit MDR

Es wird davon abgeraten, das Programm Kaspersky Endpoint Security für Linux in das Referenzabbild aufzunehmen.

Wenn Kaspersky Endpoint Security für Linux im Referenzabbild enthalten war, führen Sie auf jedem Gerät, das auf diesem Abbild basiert, folgende Schritte aus:

1. Um eine neue UUID zu erstellen, führen Sie die folgenden Befehle aus:

```
uuidgen > /var/opt/kaspersky/kesl/common/pcid
uuidgen > /var/opt/kaspersky/epagent/install_id
```

2. Deinstallieren Sie Kaspersky Endpoint Security für Linux und installieren Sie das Programm anschließend erneut.

Wenn Sie diese Schritte nicht ausführen, werden die Geräte möglicherweise nicht korrekt identifiziert.

Hochladen der KPSN-Konfigurationsdatei

Wenn Ihre Konfiguration nicht den Anforderungen für den Betrieb ohne KPSN-Konfigurationsdateien entspricht, müssen Sie für die Integration mit Kaspersky Managed Detection and Response die *KPSN-Konfigurationsdatei* auf den Administrationsserver von Kaspersky Security Center hochladen. Diese Datei enthält die notwendigen Parameter zum Übertragen der Telemetriedaten. Die KPSN-Konfigurationsdatei ist eine Datei mit pkcs7-Erweiterung und befindet sich im zip-Archiv der MDR-Konfigurationsdatei. Weitere Informationen dazu finden Sie in der Hilfe zu Kaspersky Managed Detection and Response.

Sie können die KPSN-Konfigurationsdatei in der Web Console oder in der Verwaltungskonsole hochladen.

Indem Sie die KPSN-Konfigurationsdatei laden, erklären Sie sich damit einverstanden, Daten automatisch von einem Gerät mit der installierten Anwendung 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 laden Sie die KPSN-Konfigurationsdatei in der Web Console hoch

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-Proxyservers** aus.
3. Aktivieren Sie den Schalter **KSN-Proxyserver auf dem Administrationsserver aktivieren**, um den Dienst des KSN-Proxyservers 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-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 KPSN-Konfigurationsdatei (Datei mit pkcs7-Erweiterung) aus und klicken Sie auf **Öffnen**.
8. Akzeptieren Sie die Bedingungen der KPSN-Erklärung und klicken Sie auf die Schaltfläche **Speichern**.

So laden Sie die KPSN-Konfigurationsdatei in der Verwaltungskonsole (MMC) hoch

1. Öffnen Sie in der Struktur der Verwaltungskonsole das Eigenschaftenfenster des Administrationsservers.
2. Wählen Sie den Abschnitt **KSN-Proxyserver → Einstellungen des KSN-Proxyservers** aus.
3. Aktivieren Sie das Kontrollkästchen **Administrationsserver als Proxyserver verwenden**, um den Dienst des KSN-Proxyservers zu aktivieren.
4. Aktivieren Sie das Kontrollkästchen **KPSN konfigurieren**.
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 KPSN-Konfigurationsdatei (Datei mit pkcs7-Erweiterung) aus und klicken Sie auf **Öffnen**.
8. Akzeptieren Sie die Bedingungen der KPSN-Erklärung und klicken Sie auf die Schaltfläche **Übernehmen**.

So laden Sie die KPSN-Konfigurationsdatei über die Befehlszeile hoch

Führen Sie den Befehl aus:

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

MDR-Integration konfigurieren

Vor dem Konfigurieren der Integration von Kaspersky Managed Detection and Response:

- Lassen Sie Verbindungen über die Ports 443 und 1443 zu.
- Lassen Sie Verbindungen zu den folgenden Adressen zu:
  - *.ksn.kaspersky-labs.com
  - ksn-*.kaspersky-labs.com
  - ds.kaspersky.com

  Die Liste der Adressen kann sich ändern. Um die genaue Adresse zu erhalten, können Sie sich an den Technischen Support wenden.
- Stellen Sie sicher, dass Folgendes aktiviert ist und funktioniert:
  - Kaspersky Security Network im erweiterten Modus:
  - Verhaltensanalyse.

    Um sicherzustellen, dass die Telemetriedaten vollständig sind, können Sie zusätzlich die folgenden Komponenten aktivieren: Schutz vor Web-Bedrohungen, Schutz vor Netzwerkbedrohungen, Schutz vor bedrohlichen Dateien und Schutz vor E-Mail-Bedrohungen.

Grundlegende Konfigurationsschritte

1. **Aktivieren Sie die MDR-Komponente auf eine der folgenden Arten**

   - Mithilfe eines Lizenzschlüssels.

     Fügen Sie dem Programm den MDR-Lizenzschlüssel hinzu, wenn Sie eine separate Lizenz für die Nutzung dieser Funktion erworben haben.

     Wenn Sie Kaspersky Endpoint Security im Rahmen einer Lizenz mit Kaspersky Managed Detection and Response verwenden, ist keine Aktion erforderlich.

     Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, wird der MDR-Lizenzschlüssel zur SVM hinzugefügt.

   - Mithilfe einer MDR-BLOB-Datei.

     Laden Sie in der MDR-Konsole die MDR-Konfigurationsdatei herunter. Diese Datei ist ein ZIP-Archiv, das eine MDR-BLOB-Datei und eine KPSN-Konfigurationsdatei enthält.

     Laden Sie die BLOB-Datei anschließend in die Web Console, in die Verwaltungskonsole oder über die Befehlszeile hoch.

   Die Version des Programms Kaspersky Endpoint Security bestimmt die Methode zur Aktivierung der MDR-Komponente und ob Sie die KPSN-Konfigurationsdatei verwenden müssen. Weitere Informationen dazu finden Sie in der Hilfe zu Kaspersky Managed Detection and Response.

Wenn die Administrationsserver von Kaspersky Security Center in einer Hierarchie organisiert sind und der sekundäre Server keinen direkten Internetzugang hat, kann Kaspersky Managed Detection and Response nicht funktionieren, selbst wenn der primäre Administrationsserver über einen Internetzugang verfügt.

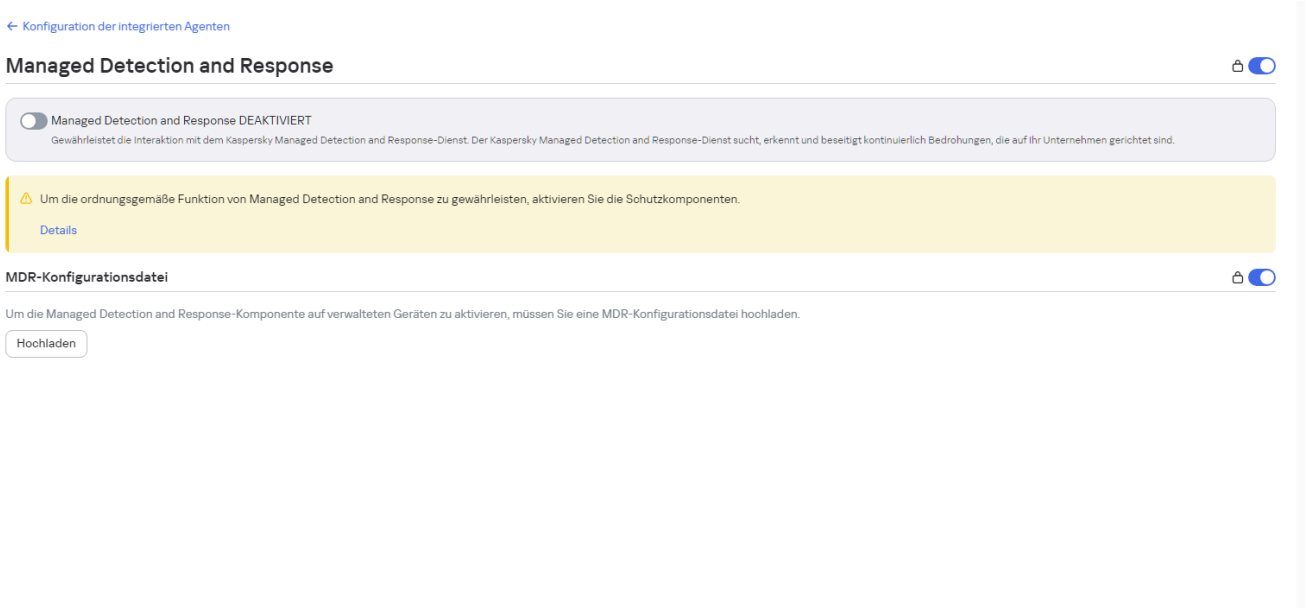
2 KPSN-Konfigurationsdatei hochladen

Wenn Ihre Organisation über mehrere Mandanten verfügt oder Sie die MDR-Komponente mithilfe eines MDR-BLOBs aktiviert haben, laden Sie die KPSN-Datei auf den Kaspersky Security Center Administrationsserver hoch. Diese Datei enthält die erforderlichen Einstellungen zum Senden von Telemetriedaten; Sie finden sie im ZIP-Archiv mit der MDR-Konfigurationsdatei.

3 Einstellungen für die Integration von Kaspersky Managed Detection and Response konfigurieren

So aktivieren Sie die Integration von Kaspersky Managed Detection and Response in der Web Console

1. Wählen Sie im Hauptfenster der Web Console den Abschnitt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf die gewünschte Kaspersky Endpoint Security-Richtlinie.
3. Wählen Sie im geöffneten Eigenschaftenfenster der Richtlinie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie im Abschnitt **Konfiguration der integrierten Agenten** die Option **Managed Detection and Response** aus und verwalten Sie dann im rechten Bildschirmbereich die folgenden Einstellungen:
   - Stellen Sie den Umschalter auf **Managed Detection and Response AKTIVIERT**.
   - Wenn Sie Mandanten haben oder die MDR-Komponente mithilfe einer MDR-BLOB-Datei aktiviert haben, klicken Sie auf die Schaltfläche **Hochladen**, um eine MDR-BLOB-Datei hinzuzufügen.
5. Speichern Sie die Einstellungen.



Managed Detection and Response

So aktivieren Sie die Integration von Kaspersky Managed Detection and Response über die Befehlszeile

1. Um die MDR-Komponente zu aktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings UseMDR=Yes
```

2. Um eine BLOB-Datei hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

4. **KSN-Richtlinie konfigurieren**

So verwalten Sie die KSN-Einstellungen in der Web Console

1. Wechseln Sie in der Kaspersky Endpoint Security-Richtlinie auf der Registerkarte **Anwendungseinstellungen** zum Abschnitt **Allgemeine Einstellungen**.
2. Wählen Sie **Kaspersky Security Network** aus und legen Sie anschließend im rechten Bildschirmbereich die folgenden Einstellungen fest:
   a. Stellen Sie den Umschalter auf **Verwendung von Kaspersky Security Network (KSN) AKTIVIERT**.
   b. Aktivieren Sie im Unterabschnitt **KSN-Einstellungen** das Kontrollkästchen **Erweiterten KSN-Modus verwenden**.
   c. Aktivieren Sie im Unterabschnitt **KSN-Proxyserver verwenden** die folgenden Kontrollkästchen:
      - **Administrationsserver als KSN-Proxyserver verwenden**
      - **Kaspersky Security Network-Server verwenden, wenn kein KSN-Proxyserver verfügbar**

   Die Telemetriedaten werden vom Administrationsserver oder vom Gerät erfasst, je nachdem, ob die konfigurierten Optionen verfügbar sind.
3. Speichern Sie die Einstellungen.

So konfigurieren Sie die KSN-Einstellungen über die Befehlszeile

Um KSN im erweiterten Modus zu aktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings UseKSN=Extended --accept-ksn
```

5. **KSN aktivieren**

So aktivieren Sie KSN in der Web Console

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.
2. Wählen Sie im geöffneten Fenster auf der Registerkarte **Allgemein** den Abschnitt **KSN-Proxy** aus.
3. Stellen Sie den Umschalter auf **KSN-Proxy auf dem Administrationsserver aktivieren Aktiviert**.

4. Aktivieren Sie je nach verwendeter KSN-Infrastrukturlösung einen Umschalter:

   - **Kaspersky Security Network verwenden Aktiviert**.
   - **Kaspersky Private Security Network verwenden Aktiviert** und laden Sie anschließend die KPSN-Konfigurationsdatei hoch.

5. Speichern Sie die Einstellungen.

6. **Stellen Sie sicher, dass die Verbindung zu Kaspersky Managed Detection and Response erfolgreich hergestellt wurde**

   Überprüfen Sie den Status von Kaspersky Managed Detection and Response auf beliebige geeignete Weise.

Überprüfen, ob die MDR-Integration aktiviert ist

Sie können die Gesundheit der Komponente Kaspersky Managed Detection and Response auf folgende Weise überprüfen:

- Über die Befehlszeile mit folgendem Befehl:

  ```
  kesl-control --app-info
  ```

  Die Integration von Kaspersky Managed Detection and Response wird mit dem Status **Verfügbar und wird ausgeführt** angezeigt.

- Wechseln Sie in der MDR-Konsole zum Abschnitt **Ressourcen**. Geräte werden mit dem Status **OK** (grün) angezeigt.

Wenn die Komponente deaktiviert ist:

1. Führen Sie ein Update der Antiviren-Datenbanken des Programms aus.
2. Stellen Sie sicher, dass Kaspersky Security Network aktiviert ist und im erweiterten Modus ausgeführt wird.
3. Überprüfen Sie die Lizenzschlüssel für Kaspersky Endpoint Security und MDR.
4. Stellen Sie sicher, dass die BLOB-Datei der Richtlinie hinzugefügt wurde.
5. Stellen Sie sicher, dass die für MDR erforderlichen Komponenten ordnungsgemäß funktionieren.

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Endpoint Security für Linux unterstützt die Lösung Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* ist eine Lösung zur Verwaltung von Sicherheitsinformationen und Ereignissen (SIEM) für die IT-Infrastruktur von Unternehmen. KUMA ermöglicht es, Sicherheitsbedrohungen zu erkennen, zu analysieren und einzudämmen, bevor sie Schaden anrichten können.

Weitere Informationen über diese Lösung finden Sie in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform.

Kaspersky Endpoint Security wird auf den einzelnen Computern einer IT-Unternehmensinfrastruktur installiert und überwacht kontinuierlich Prozesse, offene Netzwerkverbindungen und geänderte Dateien. Informationen über Ereignisse auf dem Computer (Telemetrie) werden an den Server für Kaspersky Unified Monitoring and Analysis Platform (KUMA) gesendet.

Die Komponente ist für Geräte mit Elbrus-CPU nicht verfügbar.

KUMA-Integration konfigurieren

Führen Sie vor der Konfiguration der Integration mit Kaspersky Unified Monitoring and Analysis Platform folgende Schritte aus:

- Lassen Sie Verbindungen über die Ports 443 und 1443 oder über die auf der Seite des KUMA-Kollektors konfigurierten Ports zu.
- Fügen Sie dem Programm den KUMA-Lizenzschlüssel hinzu, wenn Sie eine separate Lizenz für die Nutzung dieser Funktion erworben haben.

  Wenn Sie Kaspersky Endpoint Security mit einer Lizenz, die Kaspersky Unified Monitoring and Analysis Platform beinhaltet, verwenden, ist keine Aktion erforderlich.

  Wenn das Programm im Light Agent-Modus verwendet wird, wird der KUMA-Lizenzschlüssel zur SVM hinzugefügt.

Grundlegende Konfigurationsschritte

1. **Konfigurieren Sie in KUMA einen Kollektor und einen Normalisierer.**

   Wenn Sie ein Client-Zertifikat verwenden möchten, wählen Sie bei der Konfiguration des Kollektors auf der **Transport**-Registerkarte den Konnektortyp „tcp“ aus. Wählen Sie anschließend auf der Registerkarte **Erweiterte Einstellungen** in der **TLS-Modus**-Dropdown-Liste die Option **Benutzerdefiniertes PFX mit Client-Authentifizierung** aus.

2. **Adresse des Kollektors für die Verbindung kopieren**

   Kopieren Sie im Abschnitt **Ressourcen → Aktive Dienste** in der Diensttabelle die Werte aus den Spalten **FQDN/IP-Adresse** und **Port** und speichern Sie sie auf beliebige geeignete Weise.

   Wenn Sie TLS für die Verbindung verwenden, geben Sie nur den vollqualifizierten Domänennamen (FQDN) an. Beim Wert der Einstellung muss die Groß- und Kleinschreibung beachtet werden.

3. **Vom KUMA-Server ausgestellte Zertifikate abrufen und verarbeiten**

   Die Verwendung von Zertifikaten zum Schutz der Verbindung wird für UDP-Verbindungen zum KUMA-Server nicht unterstützt.

   Wenn in den allgemeinen Anwendungseinstellungen von Kaspersky Endpoint Security die Verwendung eines Proxyservers konfiguriert ist, wird für die Verbindung zum KUMA-Server ein Proxyserver verwendet.

Rufen Sie das Serverzertifikat (Microservice-CA-Zertifikat) ab, siehe CA-Zertifikate herunterladen. Um das Zertifikat zu verarbeiten, konvertieren Sie es in das DER- oder PEM-Format, indem Sie die Schritte im Artikel Konvertieren eines PFX-Zertifikats in das PEM-Format ausführen.

Für zusätzlichen Schutz können Sie auch ein Client-Zertifikat verwenden, das Sie bei der Konfiguration des Kollektors erhalten haben, siehe Schritt 1.

4. **Einstellungen der Integration mit Kaspersky Unified Monitoring and Analysis Platform konfigurieren**

So konfigurieren Sie die KUMA-Integration in der Kaspersky Security Center Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **KUMA-Integration**.
5. Aktivieren Sie den Umschalter **KUMA-Integration AKTIVIERT**.
6. Fügen Sie KUMA-Server hinzu:

   a. Klicken Sie auf **Hinzufügen**.

   Dadurch wird ein Formular geöffnet, in dem Sie KUMA-Server hinzufügen können.

   b. Wählen Sie das Protokoll für die Verbindung mit dem KUMA-Server aus: **HTTP/HTTPS**, **TCP**, **UDP**.

   Das Protokoll für die Verbindung mit dem Collector in Kaspersky Endpoint Security muss mit dem Connector-Typ in KUMA übereinstimmen: **http**, **tcp** oder **udp**.

   Wenn Sie das Protokoll **HTTP/HTTPS** auswählen, verwendet das Programm für die Verbindung mit KUMA-Servern standardmäßig HTTPS. Um HTTP zu verwenden, müssen Sie dieses Protokoll manuell in der Serveradresse angeben (z. B. `http://server.com`).

   c. Geben Sie die Serveradresse (IPv4, IPv6) und den Port für die Serververbindung ein (standardmäßig ist Port 443 angegeben).

   Sie können die Serveradresse in den Connector-Eigenschaften in der KUMA-Konsole einsehen. Weitere Informationen zu KUMA-Connectors finden Sie in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform.

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

   Kaspersky Endpoint Security verbindet sich mit dem ersten KUMA-Server in der Liste. Wenn die Verbindung fehlschlägt, verbindet sich Kaspersky Endpoint Security mit dem zweiten KUMA-Server in der Liste und so weiter.
7. Konfigurieren Sie, sofern erforderlich, die Einstellung **Maximale Verzögerung beim Versenden von Ereignissen (Sek.)** im Block **Einstellungen der Serververbindung**. Wenn die festgelegte Dauer abgelaufen ist, versucht Kaspersky Endpoint Security, eine Verbindung mit demselben Collector herzustellen, oder stellt eine Verbindung mit dem nächsten Collector in der Liste her, falls es mehrere Collectors gibt. Der Standardwert ist 30 Sekunden.
8. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die KUMA-Integration über die Befehlszeile

1. Um einen KUMA-Server hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 33 Servers.item_001.ServerAddress=<kuma server address>
Servers.item_001.Port=<kuma server port> Servers.item_001.ServerProtocol=<tcp|HTTPWithCompression|udp>
```

2. Um ein KUMA-Serverzertifikat hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control [-M] --add-kuma-server-certificate <path to the file>
```

3. Um die Integrationseinstellungen zu konfigurieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 33 [<setting name>=<setting value>]
```

Die Einstellungen und ihre möglichen Werte sind in der folgenden Tabelle aufgeführt.

4. Um ein Client-Zertifikat für die Verbindung mit dem Response-Server hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control [-M] --add-kuma-client-certificate <path to the file>
```

5. Um die Integration mit EDR (KATA) zu aktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --start-task 33
```

Einstellungen der Aufgabe zur Integration mit Kaspersky Unified Monitoring and Analysis Platform

Parameter	Description	Wert
`UseTls`	Aktivieren und Deaktivieren der Überprüfung des Serverzertifikats, um die Verbindung zum KUMA-Server zusätzlich abzusichern.	`Yes` – Zertifikat verwenden, um die Verbindung zum KUMA-Server zusätzlich abzusichern. `No` (Standardwert) – kein Zertifikat verwenden, um die Verbindung zum KUMA-Server abzusichern.
`UseClientCertificate`	Aktivieren und Deaktivieren der Zwei-Wege-Authentifizierung, um die Verbindung zum KUMA-Server zusätzlich abzusichern. Wenn die Überprüfung des Client-Zertifikats auf der Seite des KUMA-Servers aktiviert ist, müssen Sie die Verwendung des Client-Zertifikats aktivieren und das Client-Zertifikat hinzufügen, bevor Sie die Aufgabe "Integration mit Kaspersky Unified Monitoring and Analysis Platform" ausführen.	`Yes` – Zwei-Wege-Authentifizierung verwenden, um die Verbindung zum KUMA-Server zusätzlich abzusichern. `No` (Standardwert) – Zwei-Wege-Authentifizierung nicht verwenden.
`ConnectionTimeout`	Die maximale Wartezeit auf eine Verbindung mit dem KUMA-Server in Sekunden.	Der Standardwert ist: `5`.
Der Abschnitt **[Servers.item_#]** enthält die Parameter des KUMA-Servers.		

Parameter	Description	Wert
`ServerAddress`	Adresse des KUMA-Servers. Sie können die IP-Adresse (IPv4 oder IPv6) oder den vollqualifizierten Domänennamen (FQDN) des Servers angeben. Wenn Sie den Parameter `UseTls=Yes` festgelegt haben, müssen Sie den vollständig qualifizierten Domänennamen (FQDN) des Servers aus dem Zertifikat angeben, das Sie beim Erwerb Ihrer Lizenz zur Verwendung von KUMA erhalten haben.	Der Standardwert ist: `127.0.0.1`.
`ServerPort`	Port für die Verbindung zum KUMA-Server.	Der Standardwert ist: `443`.
`ServerProtocol`	Protokoll für die Verbindung zum KUMA-Server.	`tcp` (Standardwert) – TCP-Protokoll verwenden, um eine Verbindung zum KUMA-Server herzustellen. `HTTPWithCompression` — HTTP-Protokoll mit Ereigniskomprimierung verwenden, um eine Verbindung zum KUMA-Server herzustellen. `udp` – UDP-Protokoll verwenden, um eine Verbindung zum KUMA-Server herzustellen. Wenn das UDP-Protokoll ausgewählt ist, wird die Verwendung von Zertifikaten zum Schutz der Verbindung nicht unterstützt (die Werte der Einstellungen `UseTls`, `UseClientCertificate` und `ConnectionTimeout` werden ignoriert), und es gibt keine Ereignisse zur Verbindung mit dem KUMA-Server.
Der Abschnitt **[KumaTransferSettings]** enthält Einstellungen für die Übertragung von Ereignissen an den KUMA-Server.		
`EventTransferTimeMax`	Maximale Verzögerung beim Senden von Ereignissen an den KUMA-Server in Sekunden.	Der Standardwert ist: `30`.

5. **Stellen Sie sicher, dass die Verbindung mit Kaspersky Unified Monitoring and Analysis Platform erfolgreich hergestellt wurde**

   Überprüfen Sie den Status von KUMA auf eine beliebige geeignete Weise.

So überprüfen Sie, ob die KUMA-Integration ausgeführt wird

Sie können die KUMA-Komponente auf folgende Weise testen:

- Über die Befehlszeile mit folgendem Befehl:

  ```
  kesl-control --app-info
  ```

  Die Integration mit KUMA wird mit dem Status **Verfügbar und wird ausgeführt** angezeigt.

- In der Web Console (OSMP Console):

  Wechseln Sie zum Abschnitt **Bedrohungssuche**: In der Ereignisliste werden für das entsprechende Gerät Ereignisse mit Telemetriedaten angezeigt, die den Status "Verbindung zu KUMA wurde hergestellt" haben.

- In der Kaspersky Unified Monitoring and Analysis Platform:

  Wechseln Sie im Hauptmenü der KUMA-Konsole zum Abschnitt **Ereignisse**: In der Liste werden Ereignisse mit Telemetriedaten von Kaspersky Endpoint Security angezeigt.

Schutz virtueller Umgebungen

Kaspersky Endpoint Security unterstützt den Light Agent-Modus, um als Teil von Kaspersky Security for Virtualization Light Agent zu funktionieren. *Kaspersky Security for Virtualization Light Agent* ist eine integrierte Lösung. Sie schützt virtuelle Maschinen umfassend vor verschiedenen Bedrohungen der Informationssicherheit, Netzwerkangriffen und Phishing-Angriffen. Um diese Lösung zu verwenden, müssen Sie das Programm im Light Agent-Modus installieren.

Wenn Sie Light Agent starten, stellt Light Agent eine Verbindung zu der virtuellen Maschine SVM (Secure Virtual Machine) her und hält die Verbindung aufrecht. Auf der SVM wird ein Schutzserver bereitgestellt. Die *Schutzserver* ist eine Komponente der Lösung Kaspersky Security for Virtualization Light Agent. Sie untersucht Dateien auf Viren und andere Schadsoftware, aktualisiert die Antiviren-Datenbanken und verwaltet die Lizenzschlüssel. Light Agent sendet Dateien oder deren Fragmente, die untersucht werden müssen, an die SVM. Die Untersuchungsergebnisse sind für alle virtuellen Maschinen verfügbar, auf denen Light Agent installiert ist (SharedCache-Technologie). Diese Technologie erhöht die Effizienz der Lösung und ermöglicht eine schnellere Reaktion auf Bedrohungen.

In der Infrastruktur des Unternehmens kann es viele virtuelle Maschinen mit installiertem Light Agent und viele SVMs geben. Der Integrationsserver verwaltet die Interaktion zwischen virtuellen Maschinen und SVMs. Der *Integrationsserver* ist eine Komponente der Lösung Kaspersky Security for Virtualization Light Agent, die eine Liste der verfügbaren SVMs erstellt und diese Daten an Light Agents überträgt, an der Erkennung von SVMs durch Light Agents beteiligt ist, die Verbindung zwischen Light Agents und SVMs schützt und weitere Funktionen ausführt.

Über die Verbindung des Light Agents zur SVM

1. **Abrufen einer Liste der verfügbaren SVMs**

   Light Agent ruft die Liste der verfügbaren SVMs ab.

2. **Auswahl des optimalen Schutzservers (SVM)**

   Light Agent verwendet den Algorithmus zur SVM-Auswahl und wählt einen verfügbaren Schutzserver (SVM) aus, der optimal für die Verbindung geeignet ist.

3. **Überprüfen zusätzlicher Verbindungseinstellungen**

   Light Agent überprüft zusätzliche Einstellungen der SVM-Verbindung: Tags, Status des Verbindungsschutzes, durch die Lizenz abgedeckte Programmfunktionalität.

4. **Über die Verbindung des Light Agents zur SVM**

   Light Agent stellt eine Verbindung mit der ausgewählten SVM her und hält diese aufrecht.

So konfigurieren Sie die SVM-Erkennung

Sie können eine der Methoden zur SVM-Ermittlung für den Light Agent auswählen.

- Integrationsserver (VIIS) verwenden.

Der *Integrationsserver* ist die Komponente der Lösung, welche die Interaktion von Kaspersky Security for Virtualization Light Agent mit der virtuellen Infrastruktur ermöglicht und eine Liste der für die Verbindung verfügbaren SVMs erstellt. Light Agent stellt eine Verbindung mit dem Integrationsserver her und ruft die Liste mit SVM-Adressen ab.

Der Integrationsserver ist in großen virtuellen Infrastrukturen besonders nützlich, da er die Last zwischen den SVMs automatisch ausgleicht, Informationen über verfügbare SVMs abruft, diese Informationen analysiert und den Light Agents eine Liste der Schutzserver (SVMs) bereitstellt, die für die Verbindung optimal sind.

Damit Light Agent eine Liste mit SVMs abrufen kann, müssen Sie nur die Adresse des Integrationsservers eingeben.

- Verwenden eines Hochverfügbarkeitsclusters von Integrationsservern.

  Die Bereitstellung eines Hochverfügbarkeitsclusters von Integrationsservern ist in Kaspersky Security for Virtualization Light Agent 6.4 verfügbar. Ein Hochverfügbarkeitscluster von Integrationsservern gewährleistet den unterbrechungsfreien Schutz der virtuellen Umgebung durch das Failover von SVMs und Light Agents auf einen Backup-Integrationsserver, wenn der primäre Integrationsserver ausfällt. Eine spezielle Clusterkomponente, der *Load-Balancer*, ist für das Server-Failover verantwortlich. Einzelheiten zu einem Hochverfügbarkeitscluster von Integrationsservern finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

  Damit der Light Agent eine Liste der SVMs abrufen kann, müssen Sie die Adresse des Geräts eingeben, auf dem der Load-Balancer installiert ist.

- Liste mit SVM-Adressen verwenden.

  Wenn Sie einzelne SVMs angeben möchten, mit denen Light Agent eine Verbindung herstellen soll, können Sie manuell eine Liste erstellen.

  Sie müssen die Adressen der verfügbaren SVMs auflisten, mit denen der Light Agent eine Verbindung herstellen kann.

So konfigurieren Sie die SVM-Ermittlung durch Light Agent in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Light Agent-Modus** → **Einstellungen zur SVM-Ermittlung**.
5. Wählen Sie eine Methode zur SVM-Ermittlung aus.

   - **Integrationsserver verwenden**. Nehmen Sie abhängig von Ihrer Infrastruktur die Einstellungen für die Verbindung mit dem Integrationsserver vor:

     - **Einzelner Integrationsserver**. Geben Sie die Einstellungen für die Verbindung mit dem Integrationsserver ein: die IPv4-Adresse oder den vollqualifizierten Domänennamen (FQDN) des Geräts.

     - **Hochverfügbarkeitscluster von Integrationsservern**. Geben Sie die IP-Adresse und den Port des Load-Balancers ein, der Teil des Clusters ist.

- **Benutzerdefinierte Liste mit SVM-Adressen verwenden**. Erstellen Sie eine Liste der SVMs, mit denen Light Agent eine Verbindung herstellen kann. Geben Sie die IP-Adresse im IPv4-Format oder den vollqualifizierten Domänennamen (FQDN) des Geräts an. Jedes Listenelement muss in einer separaten Zeile eingegeben oder durch ein Semikolon (**;**) vom vorherigen Element getrennt werden.

  > In der Liste der SVM-Adressen werden nur vollständige Domänennamen (FQDN) angegeben, denen eine einzige IP-Adresse gegenübergestellt wird. Die Verwendung eines vollqualifizierten Domänennamens, der mehreren IP-Adressen entspricht, kann Fehler verursachen.

6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So zeigen Sie Informationen zur Verbindung des Light Agents mit dem Integrationsserver in der Befehlszeile an:

1. Stellen Sie sicher, dass das Programm im Light Agent-Modus installiert ist:

   ```
   kesl-control -V --ksvla-info
   ```

   Die Komponente muss den Status **Ein** haben.

2. Geben Sie Informationen zur Verbindung des Light Agents mit dem Integrationsserver 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.

So zeigen Sie Informationen zur Verbindung des Light Agents mit dem Integrationsserver in der Befehlszeile an

1. Stellen Sie sicher, dass das Programm im Light Agent-Modus installiert ist:

   ```
   kesl-control -V --ksvla-info
   ```

   Die Komponente muss den Status **Ein** haben.

2. Geben Sie Informationen zur Verbindung des Light Agents mit dem Integrationsserver 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 zur SVM-Ermittlung, die von Light Agent verwendet wird: Integrationsserver verwenden oder eine benutzerdefinierte Liste mit SVM-Adressen verwenden.
- 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.

Wie Light Agent SVMs auswählt

Die Infrastruktur des Unternehmens kann über mehrere bereitgestellte SVMs verfügen, mit denen sich Light Agents verbinden können. Um das Netzwerk und die Ressourcen der virtuellen Infrastruktur gleichmäßig auszulasten, müssen Sie die Light Agents auf die SVMs verteilen.

Algorithmen für die SVM-Auswahl

Light Agents können die folgenden Algorithmen für die SVM-Auswahl zum Herstellen der Verbindung verwenden: Standardalgorithmus (standardmäßig) und Erweiterter Algorithmus.

<table>
<tr><th>Standardalgorithmus</th><th>Erweiterter Algorithmus</th></tr>
<tr><td>Wenn dieser Algorithmus verwendet wird, wählt der Light Agent auf der virtuellen Maschine nach der Installation und dem Start eine Verbindung mit einer SVM aus, die für den Light Agent als lokal gilt.

Wenn keine lokalen SVMs gefunden werden, die für eine Verbindung geeignet sind, wählt der Light Agent die SVM aus, mit der die wenigsten Light Agents verbunden sind. Dabei bleibt die Platzierung der SVM in der virtuellen Infrastruktur unberücksichtigt.

Der Standort der SVM relativ zum Light Agent wird nicht bestimmt, wenn für den Schutzserver auf der SVM der Modus zum Schutz großer Infrastrukturen aktiviert ist. In diesem Fall wird empfohlen, den erweiterten Algorithmus der SVM-Auswahl zu verwenden und als Methode zur SVM-Ermittlung den Integrationsserver auszuwählen.

Ob eine SVM in Bezug auf den Light Agent als "lokal" gilt, wird je nach Art der virtuellen Infrastruktur ermittelt.</td><td>Wenn dieser Algorithmus angewendet wird, können Sie folgende weitere Parameter zur SVM-Auswahl angeben:

• Ob der Standort der SVM innerhalb der Infrastruktur beim Auswählen der Verbindung einer SVM berücksichtigt oder ignoriert werden soll
• Falls der SVM-Standort berücksichtigt wird, die Methode zur Bestimmung der SVM-Lokalität relativ zum Light Agent

Wenn Light Agents den SVM-Standort innerhalb der Infrastruktur ignorieren, können sich Light Agents mit allen zur Verbindung verfügbaren SVMs verbinden.

Wenn Light Agents den SVM-Standort innerhalb der Infrastruktur berücksichtigen, müssen Sie den Typ des SVM-Standorts auswählen, der bei der Ermittlung herangezogen wird, wenn eine SVM in Bezug auf den Light Agent als "lokal" gelten soll. Ob eine SVM in Bezug auf den Light Agent als "lokal" gilt, wird je nach Art der virtuellen Infrastruktur ermittelt.

Wenn Light Agents im Rahmen der Verbindungsherstellung bei der SVM-Auswahl den SVM-Standort innerhalb der Infrastruktur berücksichtigen, können Light Agents nur eine Verbindung zu jenen SVMs herstellen, die als "lokal" gelten.

Wenn Sie beispielsweise als Typ des SVM-Standorts einen Hypervisoren-Cluster angeben, gelten alle auf diesem Hypervisoren-Cluster bereitgestellten SVMs als lokal für Light Agent, und Light Agent kann sich nur mit einer dieser SVMs verbinden. Wenn in dem Cluster, in dem der Light Agent ausgeführt wird, keine SVM verfügbar ist, stellt der Light Agent keine Verbindung zu einer SVM her.

Bei der Auswahl der SVM berücksichtigen die Light Agents außerdem die Anzahl der verbundenen Light Agents, um eine gleichmäßige Zuordnung von Light Agents zu verfügbaren SVMs zu gewährleisten.

Wenn für einen Light Agent der erweiterter Algorithmus der SVM-Auswahl verwendet wird, als Methode zur SVM-Ermittlung eine Liste mit SVM-Adressen ausgewählt wurden und auf der SVM der Modus zum Schutz großer Infrastrukturen aktiviert ist, dann ist die Verbindung des Light Agents mit dieser SVM nur möglich, wenn der Light Agent den SVM-Standort ignoriert.</td></tr>
<tr><th colspan="2">Basis Dynamix Enterprise</th></tr>
<tr><td>In virtuellen Infrastrukturen auf Basis von Basis Dynamix Enterprise gilt die SVM als lokal für den Light Agent, wenn sie auf demselben Knoten bereitgestellt wurde wie die virtuelle Maschine mit installiertem Light Agent.</td><td>In virtuellen Infrastrukturen auf Basis von Basis Dynamix Enterprise kann eine SVM in einem der folgenden Fälle als lokal für Light Agent gelten:

• Die SVM wurde auf demselben Knoten bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent.
• Die SVM wurde in derselben Zone bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent.
• Die SVM wurde in demselben Rechenzentrum bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent.</td></tr>
<tr><th colspan="2">Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer und Basis Dynamix Standard</th></tr>
</table>

Standardalgorithmus	Erweiterter Algorithmus
In virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard gilt eine SVM als lokal für Light Agent, wenn sie auf demselben Hypervisor bereitgestellt wurde wie die virtuelle Maschine mit installiertem Light Agent.	In virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard kann eine SVM in einem der folgenden Fälle als lokal für Light Agent gelten: • Die SVM wurde auf demselben Hypervisor bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent. • Die SVM wurde in demselben Hypervisor-Cluster bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent. • Die SVM wurde in demselben Rechenzentrum bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent.
OpenStack und VK Private Cloud SVM	
In einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird, können Sie mithilfe des Parameters `StandardAlgorithmSvmLocality` im Abschnitt `HypervisorSpecificSettings:Openstack` der Konfigurationsdatei „appsettings.json“ des Integrationsservers festlegen, wie bestimmt wird, ob eine SVM in Bezug auf den Light Agent als lokal gilt. Je nach Version des Integrationsservers befindet sich die Datei in einem der folgenden Pfade: • /var/opt/kaspersky/viis/common/ – Datei des Linux-basierten Integrationsservers. • %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ – Datei des Windows-basierten Integrationsservers. Der Parameter `StandardAlgorithmSvmLocality` kann folgende Werte annehmen: • `ServerGroup`: Wenn dieser Wert angegeben ist, gilt eine SVM als lokal für Light Agent, wenn sie sich in derselben Servergruppe befindet wie die virtuelle Maschine mit installiertem Light Agent. Dieser Wert wird standardmäßig verwendet. • `Project`: Wenn dieser Wert angegeben ist, gilt eine SVM als lokal für Light Agent, wenn sie innerhalb desselben OpenStack-Projekts wie die virtuelle Maschine mit installiertem Light Agent bereitgestellt wurde. • `AvailabilityZone`: Wenn dieser Wert angegeben ist, gilt eine SVM als lokal für Light Agent, wenn sie sich in derselben Verfügbarkeitszone befindet wie die virtuelle Maschine mit installiertem Light Agent.	In einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird, kann eine SVM in einem der folgenden Fälle als lokal für Light Agent gelten: • Die SVM befindet sich in derselben Servergruppe wie die virtuelle Maschine mit installiertem Light Agent. • Die SVM wurde innerhalb desselben OpenStack-Projekts bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent. • Die SVM befindet sich in derselben Verfügbarkeitszone wie die virtuelle Maschine mit installiertem Light Agent.

Zusätzlich zu Algorithmen für die SVM-Verbindung können Sie die Verbindung von Light Agents mit SVMs auch mithilfe von Tags regulieren.

So konfigurieren Sie den Algorithmus zur SVM-Auswahl für Light Agent in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Light Agent-Modus** → **Algorithmus der SVM-Auswahl**.
5. Wählen Sie den Algorithmus aus:

   - **Standard-Algorithmus zur SVM-Auswahl verwenden**. Light Agent wählt SVMs aus, die im selben Hypervisor bereitgestellt werden.
   - **Erweiterten Algorithmus zur SVM-Auswahl verwenden**. Light Agent wählt SVMs aus, die an SVM-Standorten des ausgewählten Typs bereitgestellt werden (standardmäßig **Hypervisor**).

6. Wählen Sie bei Bedarf den SVM-Standort für den erweiterten Algorithmus der SVM-Auswahl aus:

- **Hypervisor**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):

  - Die SVMs werden auf demselben Hypervisor bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).

  - Die SVM befindet sich in derselben Servergruppe wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird).

  - Die SVM befindet sich auf demselben Knoten wie die virtuelle Maschine mit installiertem Light Agent (in a virtual infrastructure Basis Dynamix Enterprise).

  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 SVMs werden 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, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).

  - Die SVMs werden auf demselben OpenStack-Projekts bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird).

  - Die SVM befindet sich auf demselben Zone wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Basis Dynamix Enterprise).

  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.

- **Datencenter**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):

  - Die SVMs werden in demselben 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, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).

  - Die SVMs befinden sich in derselben Verfügbarkeitszone wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird).

  - Die SVM befindet sich in demselben Rechenzentrum wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Basis Dynamix Enterprise).

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.

- **Ignorieren**. Light Agent ignoriert den SVM-Standort für die Verbindung mit dem Schutzserver. Light Agents berücksichtigt weitere Kriterien: Tags, Anzahl der Light Agents, die mit einer SVM verbunden sind, und so weiter.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So verteilen Sie die Verbindungen von Light Agents auf SVMs

Mehrere Light Agents können sich mit einer SVM verbinden. Um die Verbindungen von Light Agents zu verteilen, können Sie eine separate Liste mit SVMs angeben. Wenn Sie einen Integrationsserver für die SVM-Ermittlung verwenden, können Sie *Tags* verwenden, um die Light Agent-Verbindungen gleichmäßig auf SVMs zu verteilen. Mithilfe eines Tags können Sie einem Light Agent eine Liste mit SVMs für die Verbindung zuweisen. Dazu müssen Sie dem Light Agent ein Tag zuweisen und dieses Tag in den SVM-Einstellungen angeben. Einzelheiten über die Angabe von Tags in den SVM-Einstellungen finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

Beispiel: Die Lösung Kaspersky Endpoint Detection and Response Optimum wird in Ihrer Infrastruktur für bestimmte Hosts der virtuellen Maschinen bereitgestellt. In diesem Fall können Sie dem Light Agent das Tag `[EDROptimum]` zuweisen, damit sich der Light Agent mit den SVMs verbindet, die über einen EDR Optimum-Lizenzschlüssel (EDR Optimum-Add-on) verfügen. Dadurch können Sie die EDR Optimum-Funktionalität auf der virtuellen Maschine mit diesem Light Agent verwenden. Wenn der Light Agent mit einer SVM ohne EDR Optimum-Lizenzschlüssel verbunden wird, ist die Funktionalität von Kaspersky Endpoint Detection and Response Optimum nicht verfügbar.

So weisen Sie ein Tag für die Verbindung zwischen SVM und Light Agent in der Web Console zu

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Light Agent-Modus** → **Tag für die Verbindung zur SVM**.
5. Aktivieren Sie das Kontrollkästchen **Tag für die Verbindung verwenden** und geben Sie ein Tag für die Verbindung zur SVM ein.

   Als Tag können Sie eine Zeichenkette von höchstens 255 Zeichen Länge eingeben. Sie können beliebige Zeichen außer dem Zeichen `;` verwenden.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Schutz der Verbindung zwischen Light Agent und einer SVM

Sie können die Verschlüsselung der Verbindung zwischen Light Agents und Schutzserver konfigurieren. Dazu müssen Sie in den Einstellungen des Schutzservers auf der SVM und in den Light Agent-Einstellungen die Verschlüsselung des Datenkanals zwischen dem Light Agent und dem Schutzserver aktivieren.

Ein Light Agent, für den der Verbindungsschutz aktiviert ist, kann sich nur mit SVMs verbinden, für die die Verschlüsselung des Datenkanals zwischen dem Light Agent und dem Schutzserver aktiviert ist. Ein Light Agent, für den der Verbindungsschutz deaktiviert ist, kann sich nur mit SVMs verbinden, für die die Kanalverschlüsselung deaktiviert ist oder für die eine unsichere Verbindung zwischen dem Schutzserver und dem Light Agent erlaubt ist.

Einzelheiten zur Konfiguration des Verbindungsschutzes auf dem Schutzserver finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

Der Schutz der Verbindung mithilfe der Verschlüsselung kann die Leistung von Kaspersky Security for Virtualization Light Agent verringern.

So konfigurieren Sie den Verbindungsschutz in einem Light Agent in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Light Agent-Modus** → **Verbindungsschutz**.
5. Aktivieren Sie das Kontrollkästchen **Datentransfer zwischen Light Agent und Schutzserver verschlüsseln**.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So ermitteln Sie den Status des Light Agent

In der Befehlszeile können Sie die folgenden Informationen über die im Light Agent-Modus verwendete App anzeigen:

- Einstellungen zur Verwendung der App im Light Agent-Modus;
- Verbindung des Light Agents zum Integrationsserver;
- Verbindung des Light Agents zur SVM.

Informationen zu den Einstellungen für die Verwendung der App im Light Agent-Modus anzeigen

```
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 oder Aus.

  Wenn der Light Agent-Modus aktiviert ist, wird das Programm als Teil der Lösung Kaspersky Security for Virtualization Light Agent verwendet.

- Modus zum Schutz der VDI-Infrastruktur: Aktiviert oder Aus.

  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 virtuellen Maschine: persistent oder nicht persistent.

- Rolle der virtuellen Maschine: Server oder Workstation.

- ID der virtuellen Maschine – UUID.

Informationen zur Verbindung des Light Agent mit dem Integrationsserver anzeigen

```
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.

Wenn in Ihrer Infrastruktur ein Failover-Cluster von Integrationsservern auf Linux-Basis bereitgestellt ist, werden die Adresse und der Port des Load Balancers angezeigt. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

Informationen zur Verbindung des Light Agent mit einer SVM anzeigen

```
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 zur SVM-Ermittlung, die von Light Agent verwendet wird: Integrationsserver verwenden oder eine benutzerdefinierte Liste mit SVM-Adressen verwenden.
- 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.

Bewährte Methoden

Bei der Bereitstellung von Kaspersky Endpoint Security für Linux können Sie die in diesem Abschnitt beschriebenen Empfehlungen verwenden, um den Computerschutz zu konfigurieren und die Leistung zu optimieren. Weitere Informationen zum Umfang mit Problemen bei der Computerleistung finden Sie in der Wissensdatenbank des Technischen Supports.

Optimierung der Ressourcenauslastung durch die Anwendung

Wenn die Anwendung mit den Standardeinstellungen ausgeführt wird, kann auf einigen Geräten die Systemleistung herabgesetzt werden. Ursache dafür ist die gemeinsame Nutzung von Systemressourcen sowohl durch Benutzeranwendungen als auch durch Kaspersky Endpoint Security.

Empfohlenes Konfigurationsszenario zur Optimierung des Systemressourcenverbrauchs durch das Programm:

1. **Verteilung der Geräte in Administrationsgruppen, die den Rollen der Geräte in der Infrastruktur entsprechen.**

   Führen Sie eine Inventarisierung der Geräte anhand der von ihnen ausgeführten Funktionen durch. Ordnen Sie die Geräte anschließend basierend auf diesen Funktionen den unterschiedlichen Administrationsgruppen zu. Verschieben Sie beispielsweise alle Webserver in eine Gruppe, alle Datenbankserver in eine weitere Gruppe und alle Workstations in eine dritte Gruppe.

2. **Konfiguration der Anwendung für typische Serverrollen**

   Konfigurieren Sie das Programm auf den Geräten wie empfohlen entsprechend ihrer Rolle in der Infrastruktur.

3. **Durchführen einer Leistungsanalyse auf Mustergeräten**

   Wählen Sie in jeder Administrationsgruppe ein oder zwei Pilotgeräte aus. Analysieren Sie für jedes Gerät, wie stark dessen Systemressourcen durch Kaspersky Endpoint Security ausgelastet werden, und wie sich die Leistung der Anwendungen ändert, die auf den Geräten installiert sind.

4. **Konfiguration der Anwendungseinstellungen auf den Mustergeräten basierend auf den Ergebnissen der Leistungsanalyse**

   Wenn die Leistung von Benutzeranwendungen erheblich nachlässt oder die Menge der von Kaspersky Endpoint Security genutzten Systemressourcen für die Ausführung des Betriebssystems und der Benutzeranwendungen kritisch ist, führen Sie die empfohlene Konfiguration des Schutzes vor bedrohlichen Dateien und der Untersuchungsaufgaben durch.

   Um die Auswirkungen der Komponenten Schutz vor Web-Bedrohungen, Schutz vor Netzwerkbedrohungen und Verhaltensanalyse auf die Leistung Ihrer Anwendungen zu verringern, optimieren Sie die Leistung dieser Komponenten.

5. **Konfiguration des Programms auf allen Geräten.**

   Wenn die oben genannten Schritte zu einer Leistungssteigerung auf den Mustergeräten führten, konfigurieren Sie die Anwendungen auf den restlichen Geräten dieses Typs auf die gleiche Weise.

Nutzung der Geräteressourcen durch die Anwendung analysieren

Bei der Untersuchung von Objekten verwendet die Anwendung Kaspersky Endpoint Security CPU-Ressourcen, die Eingabe/Ausgabe des Datenträger-Subsystems sowie den Arbeitsspeicher.

Informationen über den Ressourcenverbrauch durch das Programm anzeigen

```
top -bn1|grep kesl
```

Der Befehl muss zum Zeitpunkt der zu messenden Systemauslastung ausführt werden.

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.

Um Informationen über die Leistung des Programms zu erhalten, können Sie auch die Erfassung von Metriken für Betriebssystemressourcen konfigurieren, die vom Programm verwendet werden.

Wenn die Ausführung von Kaspersky Endpoint Security Ihr System erheblich verlangsamt, müssen Sie ermitteln, welche Komponenten und Aufgaben der Anwendung die Systemressourcen beanspruchen.

Führen Sie dazu die folgenden Experimente auf dem Gerät durch:

1. **Ressourcenverbrauch der Aufgabe "Schutz vor bedrohlichen Dateien" (Aufgabe vom Typ OAS) analysieren**

   Dadurch können Sie feststellen, ob die Leistungsprobleme mit der Aufgabe "Schutz vor bedrohlichen Dateien" oder mit Untersuchungsaufgaben (Aufgaben der Typen ODS und ContainerScan) zusammenhängen, und die Empfehlungen für die entsprechenden Aufgaben befolgen.

   So analysieren Sie den Ressourcenverbrauch der Aufgabe zum Schutz vor bedrohlichen Dateien

   1. Beenden Sie alle Untersuchungs- und Überwachungsaufgaben.
   2. Stellen Sie sicher, dass während der Analyse keine Untersuchungsaufgaben auf Befehl (Aufgaben der Typen ODS und ContainerScan) nach Zeitplan gestartet werden:
      a. Rufen Sie eine Liste aller Aufgaben des Programms ab:

      ```
      kesl-control --get-task-list
      ```

b. Rufen Sie die Zeitplaneinstellungen für alle Aufgaben der Typen ODS und ContainerScan ab:

```
kesl-control --get-schedule <task ID |name>
```

Wenn der Befehl `RuleType=Manual` ausgibt, wird die Aufgabe nur manuell ausgeführt.

c. Ändern Sie für alle Aufgaben, bei denen `RuleType` nicht `Manual` ist, den Zeitplan:

```
kesl-control --set-schedule <task ID |name> RuleType=Manual
```

3. Aktivieren Sie die Erstellung von Protokolldateien des Programms mit hohem Detaillierungsgrad:

```
kesl-control --set-app-settings TraceLevel=Detailed
```

4. Wenn die Aufgabe zum Schutz vor bedrohlichen Dateien nicht ausgeführt wird, starten Sie sie:

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

5. Belasten Sie das System in demselben Modus, der die Leistungsprobleme verursacht hat. Einige Stunden reichen aus.

6. Analysieren Sie die resultierenden Protokolldateien. Die Protokolldateien befinden sich standardmäßig im Verzeichnis /var/log/kaspersky/kesl/.

> Im Rahmen seiner Auslastung speichert die Anwendung eine große Mange an Informationen in den Protokolldateien. Dabei werden standardmäßig 10 Dateien mit je 500 MB Größe angelegt und die ältesten Informationen jeweils überschrieben.

Sollten die Probleme mit der Leistung und dem Ressourcenverbrauch weiterhin bestehen, muss der Schutz vor bedrohlichen Dateien möglicherweise optimiert werden.

Wenn keine Probleme mit der Leistung und dem Ressourcenverbrauch mehr auftreten, sind die wahrscheinlichsten Ursachen der Probleme die Untersuchungsaufgaben auf Befehl (Aufgaben der Typen ODS und ContainerScan) oder die Aufgabe zur Verhaltensanalyse. Sie müssen Untersuchungsaufgaben optimieren oder die Leistung der Aufgabe zur Verhaltensanalyse analysieren.

7. Deaktivieren Sie die Erstellung von Protokolldateien des Programms:

```
kesl-control --set-app-settings TraceLevel=None
```

2. **Analysieren Sie den Ressourcenverbrauch durch die Aufgabe zur Verhaltensanalyse (Aufgabe vom Typ Behavior_Detection).**

Auf diese Weise können Sie feststellen, ob die Leistungsprobleme mit der Aufgabe zur Verhaltensanalyse oder den Untersuchungsaufgaben (Aufgaben der Typen ODS und ContainerScan) zusammenhängen, und den Empfehlungen für die entsprechenden Aufgaben folgen.

So analysieren Sie den Ressourcenverbrauch der Aufgabe zur Verhaltensanalyse

1. Beenden Sie alle Untersuchungs- und Überwachungsaufgaben.
2. Stellen Sie sicher, dass während der Analyse keine Untersuchungsaufgaben auf Befehl (Aufgaben der Typen ODS und ContainerScan) nach Zeitplan gestartet werden:
   a. Rufen Sie eine Liste aller Aufgaben des Programms ab:

   ```
   kesl-control --get-task-list
   ```

   b. Rufen Sie die Zeitplaneinstellungen für alle Aufgaben der Typen ODS und ContainerScan ab:

   ```
   kesl-control --get-schedule <task ID|name>
   ```

   Wenn der Befehl `RuleType=Manual` ausgibt, wird die Aufgabe nur manuell ausgeführt.

   c. Ändern Sie für alle Aufgaben, bei denen `RuleType` nicht `Manual` ist, den Zeitplan:

   ```
   kesl-control --set-schedule <task ID|name> RuleType=Manual
   ```

3. Aktivieren Sie die Erstellung von Protokolldateien des Programms mit hohem Detaillierungsgrad:

   ```
   kesl-control --set-app-settings TraceLevel=Detailed
   ```

4. Wenn die Aufgabe zur Verhaltensanalyse nicht ausgeführt wird, starten Sie sie:

   ```
   kesl-control --start-task 20
   ```

5. Belasten Sie das System in demselben Modus, der die Leistungsprobleme verursacht hat. Einige Stunden reichen aus.
6. Analysieren Sie die resultierenden Protokolldateien. Die Protokolldateien befinden sich standardmäßig im Verzeichnis /var/log/kaspersky/kesl/.

   Im Rahmen seiner Auslastung speichert die Anwendung eine große Mange an Informationen in den Protokolldateien. Dabei werden standardmäßig 10 Dateien mit je 500 MB Größe angelegt und die ältesten Informationen jeweils überschrieben.

   Wenn weiterhin Probleme mit der Leistung und dem Ressourcenverbrauch auftreten, müssen Sie möglicherweise die Verhaltensanalyse optimieren.

   Wenn keine Probleme mit der Leistung und dem Ressourcenverbrauch mehr auftreten, werden die Probleme höchstwahrscheinlich von Untersuchungsaufgaben auf Befehl (Aufgaben der Typen ODS und ContainerScan) verursacht. Es sollte daher die Ausführung dieser Aufgaben optimiert werden.

7. Deaktivieren Sie die Erstellung von Protokolldateien des Programms:

   ```
   kesl-control --set-app-settings TraceLevel=None
   ```

3 Identifizieren Sie die Prozesse, deren Starts Kaspersky Endpoint Security am häufigsten erkennt

Sie können ungefährliche, häufig gestartete Prozesse von der Untersuchung ausschließen, um die Leistung der Verhaltensanalyse zu optimieren.

So ermitteln Sie die am häufigsten gestarteten Prozesse

Führen Sie den Befehl aus:

```
kesl-control --get-statistic --processes
```

Dieser Befehl gibt die Liste der Prozesse aus, deren Starts Kaspersky Endpoint Security am häufigsten erkennt, sowie die Anzahl der Starts für diese Prozesse.

4 Identifizieren Sie die Pfade, an denen Dateivorgänge am häufigsten abgefangen werden

Sie können Verzeichnisse vom Abfangen von Dateivorgängen ausschließen, um die Leistung des Schutzes vor bedrohlichen Dateien und der Untersuchungsaufgaben zu optimieren.

So erhalten Sie Informationen zum Abfangen von Dateivorgängen

Sie können Informationen zum Abfangen von Dateivorgängen auf folgende Weise abrufen:

- Rufen Sie Statistiken für Dateien ab, die von der Komponente „Schutz vor bedrohlichen Dateien“ am häufigsten untersucht werden:

  ```
  kesl-control --get-statistic --files
  ```

  Der Befehl gibt die Statistiken zu den abgefangenen Dateivorgängen der letzten 24 Stunden aus.

- Verwenden Sie die Protokolldateien des Programms für eine detailliertere Analyse. Durch einer Analyse der Protokolldateien können Sie eine Liste der Dateien bestimmen, die von der Anwendung abgefangen werden, und die Pfade identifizieren, in denen eine große Anzahl von Dateivorgängen abgefangen werden.

  Standardmäßig werden keine Protokolldateien erstellt.

  Erstellung von Protokolldateien aktivieren

  ```
  kesl-control --set-app-settings TraceLevel=Detailed
  ```

  > Das Aktivieren der Ablaufverfolgung kann sich negativ auf die Gesamtleistung des Systems auswirken. Es wird empfohlen, die Erstellung von Protokolldateien zu deaktivieren, wenn keine Notwendigkeit zur Aufzeichnung von Protokollen besteht.

  Erstellung von Protokolldateien deaktivieren

  ```
  kesl-control --set-app-settings TraceLevel=None
  ```

- Rufen Sie eine Liste der abgefangenen Dateien ab:

```
grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -F':' '{print
$2}'|sort | uniq -c | sort -k1 -n -r
```

Wenn Sie die Statistiken zum Abfangen von Dateivorgängen in Unterverzeichnissen bis zu einer bestimmten Tiefe ausgehend vom Stammverzeichnis `/` aggregieren müssen, können Sie dem Befehl `cut -d/ -f 1-X` hinzufügen, wobei X die Verschachtelungstiefe ist. Beispiel:

```
grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -F':' '{print
$2}'| cut -d/ -f 1-3|sort | uniq -c | sort -k1 -n -r|less
```

5 Identifizieren Sie die am häufigsten untersuchten Objekte

Wenn die in den vorherigen Schritten durchgeführten Maßnahmen nicht ausreichen, können Sie ungefährliche, häufig untersuchte Objekte und Dateien von der Untersuchung ausschließen, um die Leistung des Schutzes vor bedrohlichen Dateien und der Untersuchungsaufgaben zu optimieren.

Stellen Sie fest, ob die am häufigsten untersuchten Objekte gefährlich sind. Als ungefährlich können Sie zum Beispiel Datenbankdateien, Verzeichnisse und Protokolldateien festlegen, sofern deren Einträge durch einen vertrauenswürdigen Prozess vorgenommen werden. Bei Problemen wenden Sie sich an den Technischen Support.

So identifizieren Sie die am häufigsten untersuchten Objekte

1. Rufen Sie die Liste der Objekte ab, die am häufigsten untersucht wurden:

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | sort | uniq -c | sort -k1 -n -
r|less
```

Das Ergebnis wird in das Textanzeigeprogramm less geladen, wobei die Objekte, die am häufigsten untersucht wurden, zuerst angezeigt werden.

Wenn Sie die Statistiken zur Untersuchung von Objekten in Unterverzeichnissen bis zu einer bestimmten Tiefe ausgehend vom Stammverzeichnis `/` aggregieren müssen, können Sie dem Befehl `cut -d/ -f 1-X` hinzufügen, wobei X die Verschachtelungstiefe ist. Beispiel:

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | cut -d/ -f 1-4 | sort | uniq -c |
sort -k1 -n -r|less
```

2. Wenn mehrere Dienste im System häufig in Dateien schreiben, werden solche Dateien wiederholt in einer verzögerten Warteschlange untersucht. Rufen Sie die Liste der Pfade ab, die in der verzögerten Warteschlange am häufigsten untersucht wurden:

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $10}' |
sort | uniq -c | sort -k1 -n -r
```

Die Dateien, die am häufigsten untersucht wurden, werden am Anfang der Liste angezeigt.

Wenn Sie die Statistiken zur Untersuchung von Objekten in Unterverzeichnissen bis zu einer bestimmten Tiefe ausgehend vom Stammverzeichnis `/` aggregieren müssen, können Sie dem Befehl `cut -d/ -f 1-X` hinzufügen, wobei X die Verschachtelungstiefe ist. Beispiel:

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $10}' |
tr -d ',' |  cut -d/ -f 1-3 | sort | uniq -c | sort -k1 -n -r
```

Sie können die Leistung des Programms über die Befehlszeile analysieren. Wenn das Gerät durch eine

Richtlinie von Kaspersky Security Center verwaltet wird, erlauben Sie die lokale Aufgabenverwaltung, während Sie Ihre Untersuchung durchführen.

Empfehlungen für den Schutz vor bedrohlichen Dateien und die Untersuchungsaufgaben

Allgemeine Empfehlungen

Untersuchungsausnahmen

Anhand von Untersuchungsausnahmen kann ein Mittelwert zwischen Schutz und Leistung des Systems erreicht werden.

Wir empfehlen, Folgendes von der Untersuchung auszuschließen:

- Datendateien und Indexdateien von Datenbanken. Nach Einschätzung der Virenexperten von Kaspersky besteht keine Gefahr, dass sich Viren über solche Dateien verbreiten.
- Sichere Objekte aus der Liste der am häufigsten untersuchten Objekte.

Die Ausnahmen können nach Pfad (u. a. kann der Mount-Typ angegeben werden), nach Dateimaske, nach Bedrohungstyp und nach Pfad zum Prozess, der die Dateivorgänge ausführt, ausgeschlossen werden.

Die Anwendung untersucht zwar keine ausgeschlossenen Objekte, es können jedoch trotzdem minimale Verzögerungen auftreten, da die Anwendung weiterhin Dateivorgänge abfängt und blockiert. Wenn Sie selbst minimale Verzögerungen vermeiden müssen, empfehlen wir, Ausnahmen vom Abfangen von Dateioperationen zu konfigurieren.

So konfigurieren Sie Ausnahmen:

- Sie können die Ausschlüsse aus dem Schutz vor bedrohlichen Dateien innerhalb einer Richtlinie über die Web Console, die Verwaltungskonsole oder lokal auf dem Gerät anhand der Befehlszeile konfigurieren.
- Sie können Ausnahmen für Untersuchungsaufgaben vom Typ ODS und ContainerScan in den Aufgabeneinstellungen in Kaspersky Security Center oder lokal auf dem Gerät über die Befehlszeile konfigurieren.

  Ausnahmen, die für eine Untersuchungsaufgabe konfiguriert wurden, wirken sich nicht auf andere Untersuchungsaufgaben aus. Sie müssen für jede Aufgabe zur Untersuchung eigene Ausschlüsse konfigurieren.

Beispiele für über die Befehlszeile konfigurierte Ausnahmen für den Schutz vor bedrohlichen Dateien

```
Das Verzeichnis /tmp/logs sowie alle Unterverzeichnisse und Dateien rekursiv ausschließen
```

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

```
Eine bestimmte Datei oder Dateien anhand einer Maske im Verzeichnis /tmp/logs ausschließen
```

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

```
Alle Dateien mit der Erweiterung .log im Verzeichnis /tmp und in seinen Unterverzeichnissen mithilfe einer rekursiven Maske ausschließen
```

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

Ausnahmen vom Abfangen von Dateioperationen

Dateien, die von der Untersuchung ausgeschlossen sind, können von der Anwendung trotzdem im Rahmen des Schutzes vor bedrohlichen Dateien und der Untersuchungsaufgaben abgefangen werden. Die Anwendung fängt die Ereignisse der Dateivorgänge ab und blockiert die Vorgänge so lange, bis die Ereignisse verarbeitet werden. Nach einer Untersuchung kann die Anwendung:

- Die Blockade aufheben und den Vorgang zulassen.
- Den Vorgang blockieren und die Aktionen ausführen, die in den Schutz- oder Untersuchungseinstellungen angegeben wurden.

Das Abfangen von Ereignissen nimmt Zeit in Anspruch, was sich auf die Leistung anderer Anwendungen oder des Betriebssystems auswirken kann.

Wenn Ihr Betriebssystem die fanotify-Technologie unterstützt und die Anforderungen erfüllt, konfigurieren Sie das aktualisierbare Kernel-Modul für die Anwendung. Das aktualisierbare Kernel-Modul ist im Lieferumfang der Anwendung enthalten. Das aktualisierbare Kernel-Modul ermöglicht die Optimierung des Abfangens von Dateioperationen.

Um Dateien in einem bestimmten Verzeichnis nicht nur von der Untersuchung, sondern auch vom Abfangen auszuschließen, konfigurieren Sie Ausnahmen für Einhängepunkte (globale Ausnahmen). Durch das Ausschließen von Mountpunkten können Sie lokale oder Remote-Verzeichnisse, die auf dem Gerät gemountet sind, vom Modul zum Abfangen von Dateioperationen ausschließen.

Sie können die Liste der auf dem Gerät erkannten Einhängepunkte über die Web Console, die Verwaltungskonsole oder die Befehlszeile anzeigen. In der Liste werden Informationen darüber angezeigt, ob der Mountpunkt zu den Untersuchungsausnahmen hinzugefügt wurde.

Die Experten von Kaspersky empfehlen die Verwendung globaler Ausnahmen, wenn:

- die Verbindung mit einer gemounteten Remote-Ressource wie NFS oder SMB langsam ist.
- bereits minimale Verzögerungen im Systembetrieb kritisch sind.

Sie können den Typ des Einhängepunkts (Local, AllRemoteMounted, Mounted:NFS, Mounted:SMB oder Mounted:Custom) oder bestimmte Einhängepunkte angeben. Die Anwendung überwacht ausgeschlossene Bereiche nicht.

Um gemeinsam genutzte Netzwerkressourcen zu schützen, können Sie Kaspersky Endpoint Security direkt auf dem Gerät verwenden, welches die Ressourcen physisch speichert.

Wenn Sie das aktualisierbare Kernel-Modul zum Abfangen von Systemereignissen verwenden, können Sie nicht nur die gesamten Einhängepunkte, sondern auch einzelne lokale oder Remote-Verzeichnisse, die auf dem Gerät eingehängt sind, vom Abfangen ausschließen.

Wenn Sie fanotify zum Abfangen von Systemereignissen verwenden, gelten globale Ausnahmen nicht für Pfade, die keine Einhängepunkte sind.

Sie können globale Ausnahmen in einer Richtlinie über die Web Console oder die Verwaltungskonsole oder lokal auf dem Gerät über die Befehlszeile konfigurieren.

Beispiel für eine globale Ausnahme, die für das Verzeichnis /tmp über die Befehlszeile konfiguriert wurde

So schließen Sie alle Dateien im Verzeichnis /tmp vom Abfangen aus:

1. Wenn Sie fanotify zum Abfangen von Systemereignissen verwenden, überprüfen Sie, ob das Verzeichnis /tmp ein Einhängepunkt ist:

   ```
   mount
   ```

   Wenn das Verzeichnis in der Ausgabe des Befehls mount fehlt:

   a. Erstellen Sie einen Einhängepunkt:

      ```
      mount --bind /tmp/ /tmp
      ```

   b. Fügen Sie der Datei /etc/fstab die folgende Zeile hinzu, damit der neu erstellte Einhängepunkt nach dem Neustart im System erhalten bleibt:

      ```
      /tmp /tmp none defaults,bind 0 0
      ```

   Wenn Sie das aktualisierbare Kernel-Modul zum Abfangen von Systemereignissen verwenden, überspringen Sie diesen Schritt.

2. Fügen Sie das Verzeichnis /tmp den globalen Ausnahmen hinzu:

   ```
   kesl-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
   ```

3. Starten Sie die Anwendung neu, um die globalen Ausnahmen anzuwenden:

```
systemctl restart kesl
```

Begrenzen der RAM-Nutzung durch die Anwendung

Sie können die Menge des Arbeitsspeichers begrenzen, der von Kaspersky Endpoint Security bei der Untersuchung von Dateien mit der Komponente "Schutz vor bedrohlichen Dateien" und beim Ausführen von Untersuchungsaufgaben vom Typ "ODS" und "ContainerScan" verwendet wird.

Die Begrenzung des Speicherverbrauchs kann für Systeme mit großen Arbeitsspeicher (> 5 GB) nützlich sein.

Standardmäßig beträgt die Obergrenze für die Speichernutzung durch die Anwendung 8192 MB. So passen Sie die Menge des Arbeitsspeichers an, der von der Anwendung verwendet wird:

- In der Richtlinie anhand des Parameters **Begrenzung der Speichernutzung für Untersuchungsaufgaben (MB)**.
- Lokal auf dem Gerät mithilfe der Einstellung `ScanMemoryLimit` in der Konfigurationsdatei kesl.ini.

Wenn der angegebene Wert des Parameters unter 2 MB liegt, verwendet die Anwendung den Mindestwert (2 MB). Wenn der angegebene Wert die Größe des Arbeitsspeichers des Geräts übersteigt, verwendet die Anwendung maximal 25 % des Arbeitsspeichers. Dieser Wert kann nicht geändert werden.

Diese Einstellung begrenzt nur die Arbeitsspeichermenge, die bei der Untersuchung von Dateien verwendet wird. Das bedeutet, dass der gesamte Arbeitsspeicherbedarf der Anwendung den Wert dieser Einstellung überschreiten kann.

Zusätzliche Empfehlungen für den Schutz vor bedrohlichen Dateien

Nur beim Öffnen einer Datei untersuchen

Ändern des Untersuchungsmodus für Dateien, sodass Dateien nur beim Öffnen untersucht werden. Standardmäßig untersucht die Anwendung Dateien beim Öffnen und beim Schließen, wenn die Datei geändert wurde.

Sie können den Untersuchungsmodus für Dateien in den Einstellungen des Schutzes vor bedrohlichen Dateien ändern:

- In der Richtlinie mithilfe der Web Console oder der Verwaltungskonsole: Geben Sie für den Parameter **Modus für den Schutz vor bedrohlichen Dateien** den Wert **Beim Öffnen** an.
- Lokal auf dem Gerät:

```
kesl-control --set-set 1 ScanByAccessType=Open
```

Änderungen, die nach dem Öffnen an der Datei vorgenommen wurden, werden erst bei dem nächsten Zugriff auf die Datei untersucht.

Untersuchung von Archiven

Stellen Sie sicher, dass die Untersuchung von Archiven deaktiviert ist (Standardeinstellung). Das Untersuchen von Archiven verringert die Leistung, da der Zugriff auf die Archivdatei wird blockiert, bis die Datei in ein temporäres Verzeichnis entpackt und untersucht wurde. Zu den Archiven zählen sowohl herkömmliche Archive als auch gepackte Objekte wie etwa .jar-Dateien.

Sie können die Untersuchung von Archiven in der Web Console, in der Verwaltungskonsole (jeweils Parameter **Archive untersuchen**) oder lokal auf dem Gerät über die Befehlszeile (Parameter `ScanArchived`) aktivieren oder deaktivieren.

Untersuchung von aus Netzwerkverzeichnissen kopierten Dateien

Konfigurieren Sie eine Untersuchungsausnahme für Dateien, die aus Netzwerkverzeichnissen kopiert wurden. 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 Anwendung mithilfe von Kaspersky Security Center verwalten, können Sie den Ausschluss nach Prozess in der Web Console oder in der Verwaltungskonsole konfigurieren. Wenn Sie die Anwendung über die Befehlszeile verwalten, können Sie den Ausschluss nach Prozess konfigurieren, indem Sie den Abschnitt [ExcludedForProgram.item_#] zu den `[ExcludedForProgram.item_#]`.

Zusätzliche Empfehlungen für Untersuchungsaufgaben

Zeitplan für den Aufgabenstart

Einrichten des Zeitplans zur Ausführung der Untersuchungsaufgaben, so dass die Aufgaben an unterschiedlichen Zeiten gestartet werden. Die Anwendung ermöglicht das gleichzeitige Starten von Untersuchungsaufgaben, was jedoch zu erheblich gesteigertem Ressourcenbedarf führen kann. Überprüfen Sie die Zeitpläne aller Aufgaben der Typen "ODS" und "ContainerScan" entweder lokal auf dem Gerät oder in Kaspersky Security Center.

Starten Sie die Untersuchung zum Zeitpunkt der geringsten Serverauslastung.

Untersuchung von Remote-Verzeichnissen

Stellen Sie sicher, dass der Untersuchungsbereich der Untersuchungsaufgaben keine Remote-Verzeichnisse enthält, die per SMB oder NFS auf dem Gerät eingebunden sind.

Es wird stattdessen empfohlen, solche Verzeichnisse direkt auf dem Gerät zu überprüfen, das die Ressource bereitstellt. Sollte dies nicht möglich sein, vermeiden Sie das Ausführen dieser Untersuchung für Server mit kritischen Diensten, da eine solche Aufgabe relativ viel Zeit in Anspruch kann (je nach Geschwindigkeit der Verbindung und Anzahl der Dateien).

Verwendung globaler Ausnahmen und Ausnahmen für den Schutz vor bedrohlichen Dateien

Stellen Sie sicher, dass die folgenden Einstellungen für die Aufgabe zur Schadsoftware-Untersuchung aktiviert sind:

- **Globale Ausnahmen verwenden** (`UseGlobalExclusions`), um in den globalen Ausnahmen angegebene Mount-Punkte von der Untersuchung auszuschließen.
- **Ausnahmen für den Schutz vor bedrohlichen Dateien verwenden** (`UseOASExclusions`), um bei der Untersuchung die konfigurierten Ausnahmen für den Schutz vor bedrohlichen Dateien zu verwenden.

Standardmäßig sind beide Einstellungen aktiviert.

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 den Pfad für die Ausschlüsse folgendermaßen angeben: `/.snapshots/*/snapshot/`.

Empfehlungen für den Schutz vor Web-Bedrohungen und den Schutz vor Netzwerkbedrohungen

Allgemeine Empfehlungen

Firewall des Betriebssystems

Wenn im System eigene Netzwerkregeln (oder firewalld-Regeln) mit Drop-Richtlinien vorhanden sind, fügen Sie für den ordnungsgemäßen Betrieb des Programms eine Accept-Regel hinzu, um eingehende Verbindungen vom lokalen Gerät (Loopback) zuzulassen:

Beispielbefehl für iptables

```
iptables -A INPUT -i lo -j ACCEPT
```

Liste der kontrollierten Netzwerkports

Beschränken Sie die Liste der vom Programm kontrollierten Netzwerkports. Standardmäßig überwacht die Anwendung nur ausgewählte Netzwerkports. Wenn das Gerät eine SMB-Verbindung verwendet, stellen Sie sicher, dass der Standardwert verwendet wird:

- In der Richtlinie der Web Console oder der Verwaltungskonsole ist in den Parametern zur Untersuchung des Netzwerkverkehrs die Variante **Nur ausgewählte Netzwerkports überwachen** ausgewählt.
- Auf dem lokalen Gerät hat der Parameter `MonitorNetworkPort` der Untersuchung des Netzwerkverkehrs den Wert `Selected`.

Verwenden des Programms zusammen mit HAProxy

Bei Verwendung des Programms zusammen mit dem HAProxy-Load-Balancer:

1. Öffnen Sie die Konfigurationsdatei "/var/opt/kaspersky/kesl/common/kesl.ini", erstellen Sie den Abschnitt `[Environment]` und fügen Sie ihm den Parameter `TcpSynInterceptDisabled=1` hinzu.
2. Starten Sie das Programm neu:

   ```
   systemctl restart kesl
   ```

Verwenden des Programms zusammen mit Kubernetes

Damit die Komponenten „Schutz vor Web-Bedrohungen“ und „Schutz vor Netzwerkbedrohungen“ mit dem Kubernetes-Cluster mit den Netzwerk-Plug-ins Calico und Cilium zusammenarbeiten, verwalten Sie die Einstellungen `WtpFwMark`, `NtpFwMark`, `BypassFwMark` und `BypassNflogMark` in der Konfigurationsdatei kesl.ini.

Vorgehensweise, wenn der Fehler "Integritätsprüfung des Programmmoduls fehlgeschlagen" angezeigt wird

Empfehlungen für Schutz vor Web-Bedrohungen

Richtlinie zur Überprüfung von Zertifikaten

Standardmäßig entschlüsselt und untersucht die Komponente zum Schutz vor Web-Bedrohungen den Netzwerkverkehr, der über verschlüsselte Verbindungen übertragen wird. Darüber hinaus kann die Komponente das Internet verwenden, um fehlende Ketten, die zur Überprüfung des Zertifikats erforderlich sind, zu überprüfen und herunterzuladen.

Wenn das Gerät keinen direkten Internetzugang hat, führen Sie eine der folgenden Aktionen aus:

- Wählen Sie in den Einstellungen für die Untersuchung des Netzwerkverkehrs eine lokale Methode zur Zertifikatsvalidierung aus:
  - In der Richtlinie mithilfe der Web Console oder der Verwaltungskonsole: Geben Sie für den Parameter **Richtlinie zur Überprüfung von Zertifikaten** den Wert **Lokale Überprüfung** an.
  - Lokal auf dem Gerät über die Befehlszeile:

    ```
    kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
    ```

  Die Anwendung überpüft Zertifikate ohne das Internet zu verwenden.
- Konfigurieren Sie den Internetzugriff über einen Proxyserver:
  - In einer Richtlinie mithilfe der Web Console oder Verwaltungskonsole: Konfigurieren Sie die Proxy-Einstellungen.
  - Lokal auf dem Gerät über die Befehlszeile: Führen Sie folgenden Befehl aus:

    Aktivieren der Verwendung eines Proxyservers mit Authentifizierung

    ```
    kesl-control --set-app-settings UseProxy=Yes ProxyServer=<connection protocol>://<user name>:<password>@<IP address of the proxy server>:<port number>
    ```

    Aktivieren der Verwendung eines Proxyservers ohne Authentifizierung

    ```
    kesl-control --set-app-settings UseProxy=Yes ProxyServer=<connection protocol>://<IP address of the proxy server>:<port number>
    ```

Empfehlungen für Schutz vor Netzwerkbedrohungen

Kompatibilität mit REDIRECT-Regeln

So stellen Sie die Kompatibilität der Abfangregeln der Komponente „Schutz vor Netzwerkbedrohungen“ mit REDIRECT-Regeln sicher (z. B. Umleitung von Port 443 auf 8443):

1. Löschen Sie die Regel:

```
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
```

2. Ersetzen Sie sie durch die folgenden Regeln:

```
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -m mark ! --mark 0x400/0x400 -j REDIRECT --to-ports
8443
iptables -t nat -A OUTPUT -p tcp --dport 443 -m mark --mark 0x400/0x400 -m addrtype ! --src-type LOCAL -j DNAT
--to-destination :8443
```

Empfehlungen für die Verhaltensanalyse

Es wird empfohlen, die Aktivität der Prozesse, die am häufigsten von der Komponente „Verhaltensanalyse“ untersucht werden, von der Untersuchung auszuschließen.

Um herauszufinden, welche Prozesse am häufigsten gestartet werden, führen Sie den folgenden Befehl aus:

```
kesl-control --get-statistic --processes
```

Dieser Befehl gibt die Liste der Prozesse aus, deren Starts Kaspersky Endpoint Security am häufigsten erkennt, sowie die Anzahl der Starts für diese Prozesse.

Sie können Ausnahmen konfigurieren, und zwar in einer Richtlinie mithilfe der Web Console oder der Verwaltungskonsole oder lokal auf dem Gerät über die Befehlszeile.

Standardmäßig wird nur der angegebene Prozess von der Untersuchung ausgeschlossen; die Verhaltensanalyse setzt die Untersuchung der untergeordneten Prozesse eines ausgeschlossenen Prozesses fort.

Beispiele für das Konfigurieren von Ausnahmen über die Befehlszeile

Die Aktivität von my_program1 und my_program2 von der Untersuchung ausschließen

```
kesl-control --set-settings 20 UseTrustedPrograms=Yes TrustedPrograms.item_0000.ProgramPath=/bin/my_program1
TrustedPrograms.item_0001.ProgramPath=/bin/my_program2
```

Die Aktivität von my_program1 und seinen untergeordneten Prozessen von der Untersuchung ausschließen

```
kesl-control --set-settings 20 UseTrustedPrograms=Yes TrustedPrograms.item_0000.ProgramPath=/bin/my_program1
TrustedPrograms.item_0000.ApplyToDescendants=Yes
```

Interoperabilität mit Kaspersky-Lösungen

Das Programm Kaspersky Endpoint Security unterstützt die Interoperabilität mit einigen Kaspersky-Lösungen. Befolgen Sie für eine optimale Interoperabilität der Programme die Richtlinien in diesem Abschnitt.

Kaspersky Security Center Linux

Wenn Sie Kaspersky Endpoint Security für Linux zusammen mit Kaspersky Security Center 17.0 Linux verwenden, empfehlen wir, die in diesem Artikel beschriebenen Einstellungen zu verwenden.

Empfohlene Einstellungen

Programmkomponente	Empfohlener Komponentenstatus	Empfehlungen
Schutz vor bedrohlichen Dateien	Enabled	Schutzausnahmen hinzufügen: • `/opt/kaspersky/klnagent/sbin/klnagent` • `/opt/kaspersky/klnagent64/sbin/klnagent` • `/var/lib/postgresql/<PostgreSQL version>`
Schadsoftware-Untersuchung.	Enabled	Fügen Sie die Pfade zu den Verzeichnissen, die die Datenbanken enthalten, zu den globalen Ausnahmen hinzu.
Untersuchung von Wechseldatenträgern	Deaktiviert	–
Verhaltensanalyse	Enabled	Verwenden Sie die Standardeinstellungen.
Schutz vor Netzwerkbedrohungen	Enabled	Modus zum Abfangen des Netzwerkdatenverkehrs mit eBPF auswählen `NetInterceptorMode=UseEBPF`
Schutz vor Web-Bedrohungen	Enabled	Verwenden Sie die Standardeinstellungen.
Schutz vor Verschlüsselung	Deaktiviert	–
Container untersuchen	Deaktiviert	–
Inventarisierung	Deaktiviert	–
Gerätekontrolle	Deaktiviert	–
Programmkontrolle	Deaktiviert	–
Firewall.	Deaktiviert	–
Web-Kontrolle	Deaktiviert	–
Überwachung der System-Integrität	Enabled	Untersuchungsbereiche hinzufügen: • /etc • /opt/kaspersky/kesl/ • /opt/kaspersky/ksc64
Überwachung der System-Integrität	Deaktiviert	–
Endpoint Detection and Response Expert (On-Premises)	Enabled	Verwenden Sie die Standardeinstellungen.
Endpoint Detection and Response Expert (cloud)	Deaktiviert	–
Managed Detection and Response	Enabled	Verwenden Sie die Standardeinstellungen.
Network Detection and Response (KATA)	Deaktiviert	–

Programmkomponente	Empfohlener Komponentenstatus	Empfehlungen
Integration mit KUMA	Deaktiviert	–
Sandbox	Deaktiviert	–
Reaktionsaktionen	Es gelten einige Einschränkungen	Bei Reaktionsaktionen können Sie Objekte, die für Kaspersky Endpoint Security für Linux erforderlich sind, sowie kritische Systemobjekte nicht ausschließen. Stellen Sie beim Initiieren von Reaktionsaktionen sicher, dass diese das System und die von Ihnen verwendeten Anwendungen nicht beeinträchtigen.
Grafische Oberfläche	Nicht festgelegt	–
Web-Plug-in für die Verwaltung von Kaspersky Endpoint Security für Linux	Installiert	Verwenden Sie die Standardeinstellungen.
MMC-Plug-in für die Verwaltung von Kaspersky Endpoint Security für Linux	Installiert	Verwenden Sie die Standardeinstellungen.
Administrationsagent	Installiert	Verwenden Sie die Standardeinstellungen.
Mechanismus zum Abfangen von Dateioperationen	Abfangmechanismus auf Basis der fanotify-Technologie	Verwenden Sie die Standardeinstellungen.
Quelle für Systemereignis-Telemetriedaten	eBPF+auditd	`TelemetrySource=Default`
Exploit-Prävention	Deaktiviert	–
Arbeiten mit dem Kaspersky Security Network	Enabled	Verwenden Sie die Standardeinstellungen.
Schutz vor E-Mail-Bedrohungen	Enabled	Verwenden Sie die Standardeinstellungen.
Schutz vor modifizierten USB-Geräten	Deaktiviert	–
Globale Ausnahmen	Konfiguriert	Wenn Sie Kaspersky Security Center mithilfe des Schnellinstallationsskripts installieren, fügen Sie Einhängepunkte zu den Ausnahmen hinzu: `/var/lib/postgresql/<PostgreSQL version>/main` wobei `<PostgreSQL version>` die Nummer der von Ihnen verwendeten PostgreSQL-DBMS-Version ist.

Kaspersky Unified Monitoring and Analysis Platform

Wenn Sie Kaspersky Endpoint Security für Linux zusammen mit den in einem Raft-Cluster bereitgestellten Versionen 4.2 und 4.6 von Kaspersky Unified Monitoring and Analysis Platform verwenden, empfehlen wir, die in diesem Artikel beschriebenen Einstellungen zu verwenden.

Empfohlene Einstellungen

Programmkomponente	Empfohlener Komponentenstatus	Empfehlungen
Schutz vor bedrohlichen Dateien	Enabled	Schutzausnahmen hinzufügen: • `/opt/kaspersky/kuma` • `/opt/kaspersky/klnagent/sbin/klnagent` • `/opt/kaspersky/klnagent64/sbin/klnagent`
Schadsoftware-Untersuchung.	Deaktiviert	–
Untersuchung von Wechseldatenträgern	Deaktiviert	–
Verhaltensanalyse	Enabled	Prozess von der Untersuchung ausschließen `/opt/kaspersky/kuma`
Schutz vor Netzwerkbedrohungen	Enabled	Sperrung des kompromittierten Geräts deaktivieren `BlockAttackingHosts=No`

Programmkomponente	Empfohlener Komponentenstatus	Empfehlungen
Schutz vor Web-Bedrohungen	Deaktiviert	–
Schutz vor Verschlüsselung	Deaktiviert	–
Container untersuchen	Deaktiviert	–
Inventarisierung	Deaktiviert	–
Gerätekontrolle	Deaktiviert	–
Programmkontrolle	Deaktiviert	–
Firewall.	Deaktiviert	–
Web-Kontrolle	Deaktiviert	–
Überwachung der System-Integrität	Deaktiviert	–
Überwachung der System-Integrität	Deaktiviert	–
Endpoint Detection and Response Expert (On-Premises)	Deaktiviert	–
Endpoint Detection and Response Expert (cloud)	Deaktiviert	–
Managed Detection and Response	Deaktiviert	–
Network Detection and Response (KATA)	Deaktiviert	–
Integration mit KUMA	Deaktiviert	–
Sandbox	Deaktiviert	–
Reaktionsaktionen	Deaktiviert	–
Grafische Oberfläche	Nicht festgelegt	–
Administrationsagent	Installiert	Verwenden Sie die Standardeinstellungen.
Mechanismus zum Abfangen von Dateioperationen	Abfangmechanismus auf Basis der fanotify-Technologie	Verwenden Sie die Standardeinstellungen.
Quelle für Systemereignis-Telemetriedaten	eBPF+auditd	`TelemetrySource=Default`
Exploit-Prävention	Deaktiviert	–
Arbeiten mit dem Kaspersky Security Network	Enabled	Verwenden Sie die Standardeinstellungen.
Schutz vor E-Mail-Bedrohungen	Deaktiviert	–
Schutz vor modifizierten USB-Geräten	Deaktiviert	–

Referenz zu den Programmkomponenten

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 <prefix of command group>
```

wobei `<prefix of command group>` die folgenden Werte annehmen kann:

- `-A`: Befehle zur Verwaltung der Programmkontrolle
- `-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 zum Anzeigen von aktuellen Programmereignissen
- `-F`: Befehle zur Firewall-Verwaltung
- `-H`: Befehle zur Verwaltung der durch Schutz vor Verschlüsselung und Schutz vor Netzwerkbedrohungen blockierten Geräte
- `-J`: Befehle zur Verwaltung der Erfassung von Kennzahlen zur Systemleistung
- `-L`: Befehle zur Verwaltung der Lizenzschlüssel
- `-M`: Befehle zur Verwaltung der Einstellungen für die Integration der Anwendung Kaspersky Endpoint Security mit Kaspersky Unified Monitoring and Analysis Platform
- `-N`: Befehle zur Verwaltung der Einstellungen für die Untersuchung verschlüsselter Verbindungen
- `-Q`: Befehle zur Verwaltung der Quarantäne
- `-R`: Befehle zur Verwaltung der Einstellungen für die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), Kaspersky Endpoint Detection and Response Expert (cloud) und Kaspersky Endpoint Detection and Response Optimum
- `-S`: Statistische Befehle.
- `-T`: Befehle zur Verwaltung der Aufgaben und Einstellungen der Anwendung
- `-U`: Befehle zur Verwaltung von Benutzern und Rollen
- `-V`: Programmbefehle im Light Agent-Modus

- `-W`: Befehle zum Anzeigen von Ereignissen aus dem Ereignisprotokoll des Programms
- `-X`: Befehle zur Verwaltung der Einstellungen für die Integration der Anwendung Kaspersky Endpoint Security mit Sandbox

In der Bash-Shell können Sie die Autovervollständigung für die kesl-control-Befehle aktivieren.

```
Autovervollständigung für den Befehl kesl-control in der aktuellen Bash-Sitzung aktivieren

source /opt/kaspersky/kesl/shared/bash_completion.sh
```

```
Autovervollständigung für alle neuen Bash-Sitzungen aktivieren

echo "source /opt/kaspersky/kesl/shared/bash_completion.sh" >> ~/.bashrc
```

Befehle zur Verwaltung der Lizenzschlüssel

Das Präfix `-L` gibt an, dass der Befehl zur Gruppe der Befehle zur Verwaltung von Lizenzschlüsseln gehört.

> Befehle zum Hinzufügen oder Entfernen von Lizenzschlüsseln können verwendet werden, wenn das Programm im Standard-Modus oder im EDR Agent-Modus ausgeführt wird. Wenn das Programm im Light Agent-Modus verwendet wird, geben die Befehle zur Schlüsselverwaltung einen Fehler zurück.

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 Schlüssel zur Aktivierung des Programms sowie Schlüssel zur Aktivierung von Komponenten hinzufügen, die nicht durch Ihre Lizenz abgedeckt sind. Der Schlüsseltyp muss nicht im Befehl angeben werden.

```
Lizenzschlüssel mithilfe einer Schlüsseldatei hinzufügen

kesl-control [-L] --add-active-key <key file path>
```

```
Lizenzschlüssel mithilfe eines Aktivierungscodes hinzufügen

kesl-control [-L] --add-active-key <activation code>
```

Wobei gilt:

`<key file path>` ist der Pfad zur Schlüsseldatei. Wenn sich die Schlüsseldatei im aktuellen Verzeichnis befindet, ist die Angabe des Dateinamens ausreichend.

<activation code> ist der Aktivierungscode.

Beispiel für das Hinzufügen eines Schlüssels als aktiven Schlüssel mithilfe der Datei /home/test/00000001.key

```
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 Schlüssel zur Aktivierung des Programms sowie Schlüssel zur Aktivierung von Komponenten hinzufügen, die nicht durch Ihre Lizenz abgedeckt sind. Der Schlüsseltyp muss nicht im Befehl angeben werden.

Wenn der Anwendung auf dem Gerät noch kein aktiver Schlüssel hinzugefügt wurde, schlägt der Befehl fehl.

Reserve-Lizenzschlüssel mithilfe einer Schlüsseldatei hinzufügen

```
kesl-control [-L] --add-reserve-key <key file path>
```

Reserve-Lizenzschlüssel mithilfe eines Aktivierungscodes hinzufügen

```
kesl-control [-L] --add-reserve-key <activation code>
```

Wobei gilt:

<key file path> ist der Pfad zur Schlüsseldatei. Wenn sich die Schlüsseldatei im aktuellen Verzeichnis befindet, ist die Angabe des Dateinamens ausreichend.

<activation code> ist der Aktivierungscode.

Beispiel für das Hinzufügen eines Reserveschlüssels mithilfe der Datei /home/test/00000002.key

```
kesl-control --add-reserve-key /home/test/00000002.key
```

Befehl kesl-control --remove-active-key

Mit diesem Befehl können Sie einen aktiven Lizenzschlüssel löschen.

Aktiven EDR Optimum-Lizenzschlüssel löschen

```
kesl-control [-L] --remove-active-key [--edr-optimum]
```

Aktiven KUMA-Lizenzschlüssel löschen

```
kesl-control [-L] --remove-active-key [--kuma]
```

Aktiven MDR-Lizenzschlüssel löschen

```
kesl-control [-L] --remove-active-key [--mdr]
```

Aktiven Lizenzschlüssel von EDR Expert (on-premise) löschen

```
kesl-control [-L] --remove-active-key [--edr-kata]
```

Aktiven EDR Expert (cloud)-Lizenzschlüssel löschen

```
kesl-control [-L] --remove-active-key [--cxdr]
```

Aktiven KWSM-Lizenzschlüssel löschen

```
kesl-control [-L] --remove-active-key [--khcs]
```

Wobei gilt:

`--edr-optimum` – Entfernt den aktiven Lizenzschlüssel von EDR Optimum.

`--kuma` – entfernt den aktiven KUMA-Lizenzschlüssel.

`--mdr` – entfernt den aktiven MDR-Lizenzschlüssel.

`--edr-kata` – Entfernt den aktiven Lizenzschlüssel von EDR Expert (on-premise).

`--cxdr` – entfernt den aktiven EDR Expert (cloud)-Lizenzschlüssel.

`--khcs` – entfernt den aktiven KWSM-Lizenzschlüssel.

Wenn Sie in der Befehlszeile nicht die Option `--edr-optimum`, `--kuma`, `--mdr`, `--edr-kata`, `--cxdr` oder `--khcs` angeben, löscht der Befehl den aktiven Schlüssel, mit dem Ihr Programm aktiviert wurde.

Befehl kesl-control --remove-reserve-key

Mit diesem Befehl können Sie einen Reserve-Lizenzschlüssel löschen.

Reserve-EDR Optimum-Lizenzschlüssel löschen

```
kesl-control [-L] --remove-reserve-key [--edr-optimum]
```

Reserve-KUMA-Lizenzschlüssel löschen

```
kesl-control [-L] --remove-reserve-key [--kuma]
```

Reserve-MDR-Lizenzschlüssel löschen

```
kesl-control [-L] --remove-reserve-key [--mdr]
```

Reserve-Lizenzschlüssel von EDR Expert (on-premise) löschen

```
kesl-control [-L] --remove-reserve-key [--edr-kata]
```

Reserve-EDR Expert (cloud)-Lizenzschlüssel löschen

```
kesl-control [-L] --remove-reserve-key [--cxdr]
```

Reserve-KWSM-Lizenzschlüssel löschen

```
kesl-control [-L] --remove-reserve-key [--khcs]
```

Wobei gilt:

`--edr-optimum` – Entfernt den Reserve-Lizenzschlüssel von EDR Optimum.

`--kuma` – entfernt den Reserve-KUMA-Lizenzschlüssel.

`--mdr` – entfernt den Reserve-MDR-Lizenzschlüssel.

`--edr-kata` – Entfernt den Reserve-Lizenzschlüssel von EDR Expert (on-premise).

`--cxdr` – entfernt den Reserve-EDR Expert (cloud)-Lizenzschlüssel.

`--khcs` – entfernt den Reserve-KWSM-Lizenzschlüssel.

Wenn Sie in der Befehlszeile nicht die Option `--edr-optimum`, `--kuma`, `--mdr`, `--edr-kata`, `--cxdr` oder `--` angeben, entfernt der Befehl den Reserveschlüssel aus dem Programm.

Befehl kesl-control -L --query

Der Befehl gibt Informationen über die Lizenz, mit der das Programm aktiviert wurde, und die derzeit verwendeten Lizenzschlüssel aus.

```
kesl-control -L --query [--json]
```

Wobei gilt:

`--json` – Gibt Daten im JSON-Format aus.

Befehl kesl-control --load-mdr-blob

Mit dem Befehl können Sie eine BLOB-Datei auf das Gerät hochladen, die zur Integration mit Kaspersky Managed Detection and Response verwendet werden kann. Die BLOB-Datei befindet sich im ZIP-Archiv der MDR-Konfigurationsdatei.

```
kesl-control [-L] --load-mdr-blob <path to MDR BLOB file>
```

kesl-control --remove-mdr-blob

Mit dem Befehl können Sie die BLOB-Datei, die zur Integration mit Kaspersky Managed Detection and Response verwendet wird, vom Gerät entfernen.

```
kesl-control [-L] --remove-mdr-blob
```

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

Benutzerrollen verwalten

Liste der Benutzer und Rollen anzeigen

```
kesl-control [-U] --get-user-list
```

Dem angegebenen Benutzer eine Rolle zuweisen

```
kesl-control [-U] --grant-role <role> <user>
```

Benutzerrolle entziehen

```
kesl-control [-U] --revoke-role <role> <user>
```

Wobei gilt:

`<user>` ist der Name eines Benutzers oder einer Benutzergruppe.

`<role>` ist eine Rolle eines Benutzers oder einer Benutzergruppe.

Einstellungen für den Kennwortschutz

Sie können Befehle verwenden, um den Kennwortschutz zu verwalten.

Kennwortschutz aktivieren oder deaktivieren

```
kesl-control --set-permission-manager-settings Enabled=<Yes|No>
```

Aktuelle Einstellungen für den Kennwortschutz anzeigen

```
kesl-control --get-permission-manager-settings
```

Berechtigungen eines Benutzers oder einer Gruppe bearbeiten

```
kesl-control --set-permissions <user> [--group] <permissions>=<Yes|No> [--file <file name>] [--json]
```

Aktuelle Berechtigungen eines Benutzers oder einer Gruppe anzeigen

```
kesl-control --get-permissions <user> [--group] [--file <file name>] [--json]
```

Benutzer oder Benutzergruppe entfernen, für den bzw. die Berechtigungen konfiguriert sind

```
kesl-control --remove-permissions <user> [--group]
```

Wobei gilt:

`<user>` ist der Name eines Benutzers oder einer Benutzergruppe.

`<permissions>` gilt für benutzerdefinierte Berechtigungen.

Mit `--group` wird die Einstellung auf eine Benutzergruppe angewendet. Wenn diese Option nicht angegeben ist, gilt die Einstellung für einen einzelnen Benutzer.

`--file <path to file>` speichert oder exportiert Einstellungen in eine Konfigurationsdatei. Wenn diese Option nicht angegeben ist, wird das Ergebnis des Befehls in die Standardausgabe geschrieben.

`--json` – Gibt die Einstellungen im JSON-Format aus.

Richtlinie auf dem Gerät verwalten

> Um die Richtlinie auf dem Gerät zu deaktivieren, benötigt der Benutzer die Berechtigung Richtlinie von Kaspersky Security Center deaktivieren.

Wenn der Benutzer die Richtlinie auf dem Gerät deaktiviert hat, wird die Richtlinie nach einem Neustart des Geräts oder von Kaspersky Endpoint Security wieder aktiv.

```
Richtlinie auf dem Gerät deaktivieren
```

```
kesl-control --disable-policy
```

```
Richtlinie auf das Gerät anwenden
```

```
kesl-control --enable-policy
```

Verwalten von App-Aufgaben und -Einstellungen

Das Präfix `-T` gibt an, dass der Befehl zur Gruppe der Befehle zur Verwaltung von Programmeinstellungen und Aufgaben gehört.

Das Präfix `-C` kennzeichnet, dass der Befehl zur Gruppe von Befehlen zur Verwaltung der Einstellungen für die Untersuchung von Containern gehört.

Das Präfix `-N` gibt an, dass der Befehl zur Gruppe der Befehle zur Verwaltung der Einstellungen für die Untersuchung des Netzwerkverkehrs gehört.

Befehl kesl-control --export-settings

Dieser Befehl gibt alle App-Einstellungen in der Konsole aus oder exportiert sie in eine Konfigurationsdatei. Dazu gehören allgemeine Einstellungen für die Untersuchung von Containern, Einstellungen für die Untersuchung verschlüsselter Verbindungen, allgemeine App-Einstellungen und Aufgabeneinstellungen.

```
kesl-control [-T] --export-settings [--file <path to file>] [--json]
```

Wobei gilt:

`--file <path to file>` ist der vollständige Pfad zur Konfigurationsdatei, in der Sie die App-Einstellungen speichern möchten.

`--json` – Gibt die Einstellungen im JSON-Format aus.

Befehl kesl-control --import-settings

Gewähren Sie nur vertrauenswürdigen Benutzern Zugriff auf die Konfigurationsdatei. Bevor Sie Einstellungen in das Programm importieren, überprüfen Sie die Pfade zu den Verzeichnissen, Konfigurationsdateien, ausführbaren Dateien und zur Quarantäne. Importieren Sie keine Konfigurationsdateien aus nicht vertrauenswürdigen Quellen. Eine Kompromittierung der Konfigurationsdatei kann die Sicherheit, Integrität oder Funktionsfähigkeit der Infrastruktur Ihres Unternehmens sowie die Benutzerdaten beeinträchtigen.

Mit diesem Befehl können Sie alle Anwendungseinstellungen aus der Konfigurationsdatei importieren (einschließlich der allgemeinen Einstellungen für die Untersuchung von Containern, der Einstellungen für die Untersuchung verschlüsselter Verbindungen, der allgemeinen Anwendungseinstellungen und der Aufgabeneinstellungen).

```
kesl-control [-T] --import-settings --file <path to configuration file> [--json]
```

Wobei gilt:

`--file <path to file>` ist der vollständige Pfad zur Konfigurationsdatei, aus der Sie Programmeinstellungen importieren möchten.

`--json` wird angegeben, um die Einstellungen aus der Konfigurationsdatei im JSON-Format zu importieren. Wenn Sie den Schalter `--json` nicht angeben, versucht die Anwendung, 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 wird ein heruntergeladenes Update der App-Module installiert.

Befehl kann nicht ausgeführt werden, wenn die Anwendung im Light Agent-Modus ausgeführt wird.

```
kesl-control [-T] --update-application
```

Befehle zur Verwaltung der allgemeinen Anwendungseinstellungen

kesl-control --get-app-settings

Mit diesem Befehl können Sie die aktuellen Werte der allgemeinen Anwendungseinstellungen in die Konsole oder in eine Konfigurationsdatei ausgeben.

```
kesl-control [-T] --get-app-settings [--file <path to file>] [--json]
```

Wobei gilt:

`--file <path to file>` ist der Pfad zur Konfigurationsdatei, in die Sie die allgemeinen Programmeinstellungen ausgeben möchten. 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.

kesl-control --set-app-settings

Mit diesem Befehl können Sie die Werte der allgemeinen Anwendungseinstellungen mithilfe von Befehlsschaltern oder durch Importieren von Einstellungen aus einer angegebenen Konfigurationsdatei festlegen.

```
Geben Sie die Einstellungen mithilfe von Befehlszeilenoptionen an:
```

```
kesl-control [-T] --set-app-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

```
Geben Sie die Einstellungen mithilfe einer Konfigurationsdatei an:
```

```
kesl-control [-T] --set-app-settings --file <path to file> [--json]
```

Wobei gilt:

`<setting name>=<setting value>` ist der Name und Wert einer allgemeinen Programmeinstellung.

`--file <path to file>` ist der vollständige Pfad zur Konfigurationsdatei, aus der Sie Programmeinstellungen importieren möchten.

`--json` wird angegeben, um die Einstellungen aus der Konfigurationsdatei im JSON-Format in die App zu importieren. Wenn Sie den Schalter `--json` nicht angeben, versucht die Anwendung, 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.

```
kesl-control [-T] --get-settings <task ID|name> [--file <path to file>] [--json]
```

Wobei gilt:

`<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`--file <path to file>` ist der Pfad zur Konfigurationsdatei, in die Sie die Aufgabeneinstellungen ausgeben möchten. 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.

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.

Geben Sie die Einstellungen mithilfe von Befehlszeilenoptionen an:

```
kesl-control [-T] --set-settings <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>] [-
-add-path <path>] [--del-path <path>] [--add-exclusion <path>] [--del-exclusion <path>]
```

Geben Sie die Einstellungen mithilfe einer Konfigurationsdatei an:

```
kesl-control [-T] --set-settings <task ID/name> --file <path to file> [--json]
```

Wobei gilt:

`<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`<setting name>=<setting value>` ist der Name und der Wert einer Aufgabeneinstellung.

`--add-path <path>` fügt einen Pfad zu einem Verzeichnis mit zu untersuchenden Objekten hinzu.

`--del-path <path>` entfernt einen Pfad zu einem Verzeichnis mit zu untersuchenden Objekten.

`--add-exclusion <path>` fügt einen Pfad zu einem Verzeichnis mit Objekten hinzu, die von der Untersuchung ausgeschlossen werden sollen.

`--del-exclusion <path>` entfernt einen Pfad zu einem Verzeichnis mit Objekten, die von der Untersuchung ausgeschlossen werden sollen.

`--file <path to file>` ist der vollständige Pfad zur Konfigurationsdatei, aus der Sie die Aufgabeneinstellungen importieren möchten.

`--json` wird angegeben, um die Einstellungen aus der Konfigurationsdatei im JSON-Format zu importieren. Wenn Sie den Schalter `--json` nicht angeben, versucht die Anwendung, 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.

```
kesl-control [-T] --set-settings <task ID|name> --set-to-default
```

Wobei gilt:

`<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

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.

```
kesl-control [-T] --get-schedule <task ID|name> [--file <path to file>] [--json]
```

Wobei gilt:

`<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`--file <path to file>` ist der Pfad zur Konfigurationsdatei, in die Sie die Einstellungen des Aufgabenzeitplans ausgeben möchten. 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.

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.

Geben Sie die Einstellungen mithilfe von Befehlszeilenoptionen an:

```
kesl-control [-T] --set-schedule <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

Geben Sie die Einstellungen mithilfe einer Konfigurationsdatei an:

```
kesl-control [-T] --set-schedule <task ID|name> --file <path to file> [--json]
```

Wobei gilt:

`<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`<setting name>=<setting value>` ist der Name und der Wert einer Einstellung des Aufgabenzeitplans.

`--file <path to file>` ist der vollständige Pfad zur Konfigurationsdatei, aus der Sie die Einstellungen des Aufgabenzeitplans importieren möchten.

`--json` wird angegeben, um die Einstellungen aus der Konfigurationsdatei im JSON-Format zu importieren. Wenn Sie den Schalter `--json` nicht angeben, versucht die Anwendung, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Befehle zur Aufgabenverwaltung

kesl-control --get-task-list

Dieser Befehl gibt eine Liste vorhandener Aufgaben aus.

```
kesl-control [-T] --get-task-list [--json]
```

Wobei gilt:

`--json` – Gibt die Einstellungen im JSON-Format aus.

Für jede Aufgabe werden folgende Informationen angezeigt:

- `Name` – Aufgabenname.
- `ID` – Aufgaben-ID.

- `Type` – Aufgabentyp.
- `State`: der aktuelle Status der Aufgabe

Wenn die Kaspersky Security Center-Richtlinie Benutzern das Anzeigen und Bearbeiten lokaler Aufgaben verbietet, sind Informationen zu den Aufgaben `Scan_My_Computer`, `Critical_Areas_Scan`, `Container_Scan`, `Inventory_Scan`, `Update` und `Rollback` nicht verfügbar.

Befehl kesl-control --get-task-state

Mit diesem Befehl wird der Status der angegebenen Aufgabe ausgegeben.

```
kesl-control [-T] --get-task-state <task ID|name> [--json]
```

Wobei gilt:

`<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`--json` – Gibt die Einstellungen im JSON-Format aus.

Aufgaben der App können folgende Status haben:

- `Started` – Aufgabe wird ausgeführt.
- `Starting` – Aufgabe wird gestartet.
- `Stopped` – Aufgabe wurde gestoppt.
- `Stopping` – Aufgabe wird gestoppt.

Aufgaben der Typen `ODS`, `ODFIM` und `InventoryScan` können außerdem einen der folgenden Status haben:

- `Pausing` – Aufgabe wird angehalten.
- `Suspended` – Aufgabe wurde angehalten.
- `Resuming` – Aufgabe wird fortgesetzt.

Befehl kesl-control --create-task

Mit diesem Befehl wird eine Aufgabe des angegebenen Typs mit den Standardeinstellungen oder mit den in einer Konfigurationsdatei angegebenen Einstellungen erstellt.

Es können nur Benutzeraufgaben erstellt werden. Vordefinierte Aufgaben können nicht erstellt werden.

Je nach Modus des Programms können Sie die folgenden Arten von Benutzeraufgaben erstellen:

- Standard-Modus: `ODS`, `Update`, `Rollback`, `ODFIM`, `ContainerScan` und `InventoryScan`.
- Light Agent-Modus: `ODS`, `ODFIM`, `ContainerScan` und `InventoryScan`.

Aufgabe mit Standardeinstellungen erstellen

```
kesl-control [-T] --create-task <task name> --type <task type>
```

Aufgabe mit Einstellungen aus einer Konfigurationsdatei erstellen

```
kesl-control [-T] --create-task <task name> --type <task type> [--file <path to file>] [--json]
```

Wobei gilt:

`<task name>` ist ein Name, den Sie für eine neue Aufgabe angegeben haben.

`<task type>` gibt den Aufgabentyp an, den Sie erstellen möchten.

`--file <path to file>` ist der vollständige Pfad zur Konfigurationsdatei mit den Einstellungen, die zum Erstellen der Aufgabe verwendet werden.

`--json` wird angegeben, um die Einstellungen aus der Konfigurationsdatei im JSON-Format zu importieren. Wenn Sie den Schalter `--json` nicht angeben, versucht die Anwendung, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Befehl kesl-control --delete-task

Dieser Befehl löscht eine Aufgabe.

Es können nur Benutzeraufgaben gelöscht werden. Vordefinierte Aufgaben können nicht erstellt werden.

```
kesl-control [-T] --delete-task <task ID|name>
```

Wobei gilt:

`<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Befehl kesl-control --start-task

Mit diesem Befehl wird eine Aufgabe gestartet.

Sie können alle vordefinierten Aufgaben und Benutzeraufgaben starten und beenden, mit Ausnahme von Aufgaben des Typs `License`.

```
kesl-control [-T] --start-task <task ID|name> [-W] [--progress]
```

Wobei gilt:

`<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`-W` – Ausgabe aktueller Ereignisse aktivieren.

`--progress` – Fortschritt der laufenden Aufgabe anzeigen.

Beispiel für das Ausführen einer Aufgabe mit der ID 1 und das Aktivieren der Anzeige aktueller Ereignisse, die mit der Aufgabe verbunden sind

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

Wenn beim Starten einer Aufgabe ein Fehler auftritt und die Aufgabe nicht gestartet wird, erfolgt nach einem Neustart der Anwendung ein erneuter Versuch, die Aufgabe zu starten.

Befehl kesl-control --stop-task

Mit diesem Befehl wird eine Aufgabe beendet.

Sie können alle vordefinierten Aufgaben und Benutzeraufgaben starten und beenden, mit Ausnahme von Aufgaben des Typs `License`.

```
kesl-control [-T] --stop-task <task ID|name> [-W]
```

Wobei gilt:

`<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`-W` – Ausgabe aktueller Ereignisse aktivieren.

Befehl kesl-control --suspend-task

Mit diesem Befehl wird eine Aufgabe angehalten.

Sie können nur Aufgaben der Typen `ODS`, `ODFIM` und `InventoryScan` anhalten.

```
kesl-control [-T] --suspend-task <task ID|name>
```

Wobei gilt:

`<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Befehl kesl-control --resume-task

Mit diesem Befehl wird die Ausführung einer Aufgabe fortgesetzt.

Sie können nur Aufgaben der Typen `ODS`, `ODFIM` und `InventoryScan` fortsetzen.

```
kesl-control [-T] --resume-task <task ID|name>
```

Wobei gilt:

`<task ID|name>` ist die ID, die der Aufgabe zum Zeitpunkt ihrer 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.

```
kesl-control [-T] --scan-file <path> [--action <action>]
```

Wobei gilt:

`<path>` ist der Pfad zu der Datei oder dem Verzeichnis, die bzw. das Sie untersuchen möchten. Sie können mehrere, durch Leerzeichen getrennte Pfade angeben.

`--action <action>` ist die Aktion, die das Programm für infizierte Objekte ausführen soll. Wenn Sie den Schalter `--action` nicht angeben, führt die Anwendung die empfohlene Aktion aus.

Befehl kesl-control --scan-container

Mit diesem Befehl können Sie eine Aufgabe des Typs Benutzerdefinierte Untersuchung von Containern oder von Images erstellen und starten.

```
kesl-control [-T] --scan-container <ID|name[:tag]>
```

Wobei gilt:

`<ID|name[:tag]>` ist der Name oder die ID des Containers oder Images. Bei der Untersuchung mehrerer Objekte können Masken verwendet werden.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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

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.

```
kesl-control [-C] --get-container-settings [--file <path to file>] [--json]
```

Wobei gilt:

`--file <path to file>` ist der Pfad zur Konfigurationsdatei, in die Sie die allgemeinen Einstellungen für die Untersuchung von Containern ausgeben möchten. 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.

kesl-control --set-container-settings

Mit diesem Befehl können Sie die Werte der allgemeinen Einstellungen für die Untersuchung von Containern mithilfe von Befehlsschaltern oder durch Importieren von Einstellungen aus einer angegebenen Konfigurationsdatei festlegen.

Geben Sie die Einstellungen mithilfe von Befehlszeilenoptionen an:

```
kesl-control [-C] --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Geben Sie die Einstellungen mithilfe einer Konfigurationsdatei an:

```
kesl-control [-C] --set-container-settings --file <path to file> [--json]
```

Wobei gilt:

`<setting name>=<setting value>` ist der Name und Wert einer allgemeinen Einstellung für die Untersuchung von Containern.

`--file <path to file>` ist der vollständige Pfad zur Konfigurationsdatei, aus der Sie die allgemeinen Einstellungen für die Untersuchung von Containern importieren möchten.

`--json` wird angegeben, um die Einstellungen aus der Konfigurationsdatei im JSON-Format in die App zu importieren. Wenn Sie den Schalter `--json` nicht angeben, versucht die Anwendung, 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 des Netzwerkverkehrs

Das Präfix `-N` gibt an, dass der Befehl zur Gruppe der Befehle zur Verwaltung der Einstellungen für die Untersuchung des Netzwerkverkehrs gehört.

Befehl kesl-control -N --query

Mit diesem Befehl können Sie Listen mit Ausschlüssen von der Untersuchung verschlüsselter Verbindungen ausgeben:

- Liste der vom Benutzer hinzugefügten Ausschlüsse.
- Liste der von der Anwendung hinzugefügten Ausschlüsse.
- Liste der von den Anwendungsdatenbanken abgerufenen Ausschlüsse.

```
Liste der vom Benutzer hinzugefügten Ausnahmen anzeigen
```

```
kesl-control -N --query user
```

```
Liste der von der App hinzugefügten Ausnahmen anzeigen
```

```
kesl-control -N --query auto
```

```
Liste der aus den App-Datenbanken erhaltenen Ausnahmen anzeigen
```

```
kesl-control -N --query kl
```

Befehl kesl-control --clear-web-auto-excluded

Mit diesem Befehl können Sie die Liste der Domänen löschen, welche die Anwendung automatisch von der Untersuchung ausgeschlossen hat.

```
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 des Netzwerkverkehrs in die Konsole oder in eine Konfigurationsdatei ausgeben.

```
kesl-control [-N] --get-net-settings [--file <path to file>] [--json]
```

Wobei gilt:

`--file <path to file>` ist der Pfad zur Konfigurationsdatei, in die Sie die Einstellungen für die Untersuchung des Netzwerkverkehrs ausgeben möchten. 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.

Befehl kesl-control --set-net-settings

Mit diesem Befehl können Sie die Werte der Einstellungen für die Untersuchung des Netzwerkverkehrs mithilfe von Befehlsschaltern oder durch Importieren von Einstellungen aus einer angegebenen Konfigurationsdatei festlegen.

Geben Sie die Einstellungen mithilfe von Befehlszeilenoptionen an:

```
kesl-control [-N] --set-net-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Geben Sie die Einstellungen mithilfe einer Konfigurationsdatei an:

```
kesl-control [-N] --set-net-settings --file <path to file> [--json]
```

Wobei gilt:

`<setting name>=<setting value>` ist der Name und der Wert einer Einstellung für die Untersuchung des Netzwerkverkehrs.

`--file <path to file>` ist der vollständige Pfad zur Konfigurationsdatei, aus der Sie die Einstellungen für die Untersuchung des Netzwerkverkehrs importieren möchten.

`--json` wird angegeben, um die Einstellungen aus der Konfigurationsdatei im JSON-Format in die App zu importieren. Wenn Sie den Schalter `--json` nicht angeben, versucht die Anwendung, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

kesl-control --list-certificates

Mit diesem Befehl können Sie die Liste vertrauenswürdiger Stammzertifikate ausgeben.

```
kesl-control [-N] --list-certificates
```

Befehl kesl-control --add-certificate

Mit dem Befehl können der Liste mit vertrauenswürdigen Stammzertifikaten ein Zertifikat hinzufügen.

```
kesl-control [-N] --add-certificate <path to certificate>
```

Wobei gilt:

`<path to certificate>` ist der Pfad zur 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 Stammzertifikate entfernen.

```
kesl-control [-N] --remove-certificate <certificate subject>
```

Befehl kesl-control --add-bypass-endpoints

Mit dem Befehl können Sie dem Abfangen des Datenverkehrs eine Ausnahme hinzufügen.

```
kesl-control [-N] --add-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

Wobei gilt:

`<in|out>` ist die Richtung des Datenverkehrs in der als Ausnahme festgelegten Verbindung: ausgehend oder eingehend.

`<remote IP address>` ist die IPv4- oder IPv6-Adresse des Remote-Geräts. Beim Ausschließen eingehenden Datenverkehrs wird der Datenverkehr von der angegebenen IP-Adresse ausgeschlossen. Beim Ausschließen ausgehenden Datenverkehrs wird der Datenverkehr zu der angegebenen IP-Adresse ausgeschlossen.

`<destination port>` ist ein Port auf dem geschützten Gerät (Ausnahme für eingehenden Datenverkehr) oder ein Port auf dem Remote-Gerät (Ausnahme für ausgehenden Datenverkehr). Der Datenverkehr an diesem Port wird vom Abfangen ausgeschlossen.

Befehl kesl-control --list-bypass-endpoints

Mit dem Befehl können Sie die Liste der konfigurierten Ausnahmen vom Abfangen des Datenverkehrs anzeigen.

```
kesl-control [-N] --list-bypass-endpoints
```

Befehl kesl-control --remove-bypass-endpoints

Mit dem Befehl können Sie eine Ausnahme aus dem Abfangen des Datenverkehrs löschen.

```
kesl-control [-N] --remove-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

Wobei gilt:

`<in|out>` ist die Richtung des Datenverkehrs in der als Ausnahme festgelegten Verbindung: ausgehend oder eingehend.

`<remote IP address>` ist die IPv4- oder IPv6-Adresse des Remote-Geräts, dessen Datenverkehr von der Überprüfung ausgenommen ist (abhängig von der Richtung des Datenverkehrs).

`<destination port>` ist ein Port auf dem geschützten Gerät (Ausnahme für eingehenden Datenverkehr) oder ein Port auf dem Remote-Gerät (Ausnahme für ausgehenden Datenverkehr).

Status- und Schutzüberwachung

Statistikbefehle

Das Präfix -S gibt an, dass der Befehl zur Befehlsgruppe Statistik gehört.

kesl-control --app-info

Mit diesem Befehl können Sie Informationen zur Anwendung ausgeben.

```
kesl-control [-S] --app-info [--json] [--check-permissions]
```

Wobei gilt:

`--json` – Gibt die Einstellungen im JSON-Format aus.

`--check-permissions` zeigt Pfade zu Programmverzeichnissen mit falsch konfigurierten Berechtigungen an.

Befhel kesl-control --supported-tech-info

Dieser Befehl zeigt eine Liste der Programmfunktionen, Informationen zu deren Status (verwendet oder nicht verwendet) und die Linux-Technologien an, mit denen diese Programmfunktionen implementiert sind.

```
kesl-control [-S] --supported-tech-info [--json]
```

Wobei gilt:

`--json` – Gibt die Funktionen im JSON-Format aus.

Befehl kesl-control --get-statistic

Mit dem Befehl können Sie Statistiken über die Anwendungsausführung und eine Liste der auf dem Gerät erkannten Mountpunkte anzeigen.

```
kesl-control [-S] --get-statistic [--files] [--processes] [--mountpoints]
```

Wobei gilt:

`--files` – Statistiken über Dateien, die von der Komponente Schutz vor bedrohlichen Dateien am häufigsten untersucht werden, und die Häufigkeit, mit der die Komponente auf diese Dateien zugreift.

`--processes` – Statistiken über die Prozesse, deren Starts Kaspersky Endpoint Security am häufigsten erkennt, und die Anzahl dieser Starts.

> Das Ausschließen von Prozessen aus der Untersuchung durch die Verhaltensanalyse entfernt die Prozesse nicht aus den Statistiken, verbessert aber die Leistung von Kaspersky Endpoint Security.

`--mountpoints`: Liste der Einhängepunkte. Die Ausgabe werden die Pfade zu den Mountpunkten (MP) wie folgt sortiert:

- statische MP, System-MP, Service-MP und andere MP
- gemountete Snap-Pakete und MP innerhalb deren Namensräume
- Vom Docker-Containerverwaltungssystem erstellte Einhängepunkte

Sie können sowohl einen oder mehrere Parameter in beliebiger Kombination als auch gar keinen Parameter angeben. Wenn Sie keinen Parameter angeben, gibt die Anwendung drei Listen aus: Statistik über die am häufigsten untersuchten Dateien, Statistik über die am häufigsten gestarteten Prozesse und eine Liste der auf dem Gerät erkannten Mountpunkte.

Befehl kesl-control --omsinfo

Mit diesem Befehl können Sie eine Datei im JSON-Format für die Integration mit der Microsoft Operations Management Suite erstellen.

```
kesl-control [-S] --omsinfo --file <path to file>
```

Befehl zur Anzeige von Ereignissen

Das Präfix `-W` kennzeichnet einen Befehl zur Anzeige von Ereignissen aus dem Ereignisprotokoll des Programms.

kesl-control -W

Der Befehl aktiviert die Ausgabe aktueller Anwendungsereignisse. Der Befehl gibt den Namen des Ereignisses und zusätzliche Informationen über das Ereignis zurück. Mit diesem Befehl können Sie alle aktuellen Anwendungsereignisse oder nur Ereignisse ausgeben, die mit der ausgeführten Aufgabe verknüpft sind.

```
kesl-control -W [--query "<filter conditions>"]
```

Wobei gilt:

`<filter conditions>` gibt einen oder mehrere logische Ausdrücke im Format `<field> <comparison operation> '<value>'` an, die mit dem logischen Operator `and` kombiniert werden, um bestimmte aktuelle Ereignisse auszugeben.

Befehle zur Verwaltung der Ereignisse der Anwendung

Das Präfix -E gibt an, dass der Befehl zur Gruppe der Befehle zur Verwaltung der Anwendungsereignisse gehört.

kesl-control -E

Mit diesem Befehl können Sie Informationen zu allen Ereignissen aus dem Ereignisprotokoll der Anwendung ausgeben. Mit dem Tool `less` können Sie durch die Liste der angezeigten Ereignisse navigieren.

```
kesl-control -E
```

Befehl kesl-control -E --query

Mit diesem Befehl können Sie Informationen zu Ereignissen aus dem Ereignisprotokoll der Anwendung 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.

```
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] [--file <path to file>] [--
json] [--reverse]
```

Wobei gilt:

`<database file>` ist der vollständige Pfad zur Datenbankdatei des Ereignisprotokolls, aus der Ereignisse ausgegeben werden sollen. 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 Programmeinstellung `EventsStoragePath` bestimmt.

`<filter conditions>` gibt einen oder mehrere logische Ausdrücke im Format `<field> <comparison operator> '<value>'` an, die mit dem logischen Operator `and` kombiniert werden, um die Ergebnisse der Abfrage einzuschränken.

`<number>` ist die Anzahl der neuesten Ereignisse in der Auswahl (d. h. die Anzahl der Datensätze, gezählt ab dem Ende der Auswahl), die Sie ausgeben möchten.

`--file <path to file>` ist der vollständige Pfad zu der Datei, in die Ereignisse ausgegeben werden sollen. 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).

Befehl zum Verwalten von Systemleistungsmetriken

Befehl kesl-control --export-metrics

Mit dem Befehl können Sie die Sammlung von Kennzahlen zum Status des Betriebssystems konfigurieren.

```
kesl-control [-J] --export-metrics [--period <interval in seconds between exports>|--interactive]
```

Wobei gilt:

`--period` – periodisches Intervall für die Ausgabe der Ergebnisse an die Befehlszeile

`<interval in seconds between exports>` gibt an, wie oft die Befehlsergebnisse in der Befehlszeilenkonsole ausgegeben werden (in Sekunden)

`--interactive` – interaktive Ausgabe (durch Drücken der **`Eingabetaste`**)

Sicherheitskontrolle

Befehle zur Verwaltung der Gerätekontrolle

Das Präfix -D gibt an, dass der Befehl zur Gruppe der Befehle zur Verwaltung der Gerätekontrolle gehört.

Verwalten der Einstellungen der Gerätekontrolle

Aktuelle Einstellungen der Gerätekontrolle anzeigen

```
kesl-control --get-settings 15 [--file <path to file>] [--json]
```

Einstellungen der Programmkontrolle ändern

```
kesl-control --set-settings 15 [<setting>=<value>] [--file <path to file>] [--json]
```

Wobei gilt:

`<setting>=<value>` gibt eine Einstellung der Gerätekontrolle und ihren Wert an.

--file <path to file> speichert oder exportiert Einstellungen in eine Konfigurationsdatei. Wenn diese Option nicht angegeben ist, wird das Ergebnis des Befehls in die Standardausgabe geschrieben.

`--json` – Gibt Daten im JSON-Format aus.

Geräteverwaltung

Liste der angeschlossenen Geräte anzeigen

```
kesl-control [-D] --get-device-list [--all] [--json] [--export <file>]
```

Wobei gilt:

`--all` – Gibt eine Liste aller verbundenen Geräte aus.

`--json` – Gibt eine Liste aller verbundenen Geräte im JSON-Format aus.

`--export <file>` exportiert die Liste der angeschlossenen Geräte in eine JSON-Datei. Die Liste der angeschlossenen Geräte wird exportiert.

Kaspersky Endpoint Security zeigt folgende Informationen zu den angeschlossenen Geräten an:

- **Gerätetyp**. Der Typ des angeschlossenen Geräts. Beispielsweise `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).
- **Bus**. Verbindungsbus. Mögliche Werte: `UnknownBus`, `USB`, `FireWire`.
- **Treiber**. Der Name des zu verwendenden Treibers, wie er vom virtuellen Betriebssystem sysfs gelesen wird.

Vertrauenswürdige Geräte

Mit diesem Befehl können Sie die Liste der vertrauenswürdigen Geräte anzeigen, Geräte zur Liste hinzufügen und daraus entfernen sowie die Liste der vertrauenswürdigen Geräte aus einer Datei importieren.

```
kesl-control [-D] --trusted-devices [--list] [--add <ID>] [--delete <ID>] [--merge|--add|--replace --file <file>]
```

Wobei gilt:

`--list` – Gibt eine Liste der vertrauenswürdigen Geräte aus.

`--add <ID>` fügt ein Gerät nach Geräte-ID oder Geräte-ID-Maske zur Liste der vertrauenswürdigen Geräte hinzu.

`--delete <ID>` entfernt ein Gerät nach Geräte-ID oder Geräte-ID-Maske aus der Liste der vertrauenswürdigen Geräte.

`--merge` – Vereinigt die Listen der vertrauenswürdigen Geräte beim Import. Wenn die aktuelle Liste und die importierte Liste Einträge für ein Gerät mit der gleichen ID enthalten, werden die Parameter des vorhandenen Eintrags geändert. Für Geräte, die sich noch nicht in der aktuellen Liste befinden, werden Einträge hinzugefügt.

`--add` – Ergänzt die aktuelle Liste der vertrauenswürdigen Geräte beim Import. Es werden nur die Einträge für Geräte hinzugefügt, die zuvor nicht in der Liste enthalten waren.

`--replace` – Ersetzt die aktuelle Liste der vertrauenswürdigen Geräte. Die bestehende Liste vertrauenswürdiger Geräte wird durch die importierte Liste ersetzt.

`--file <file>` importiert eine Liste vertrauenswürdiger Geräte aus der angegebenen Datei. Sie müssen den vollständigen Pfad zur Datei im JSON-Format angeben.

Temporärer Zugriff auf ein blockiertes Gerät

Mit den Befehlen können Sie eine Zugriffsanfragedatei erstellen und einen Zugriffsschlüssel hochladen, um vorübergehenden Zugriff auf ein gesperrtes Gerät zu erhalten:

Zugriffsanfragedatei erstellen

```
kesl-control [-D] --request-temporary-device-access --device-id <device ID> --access-duration <access duration> --
path <path to access request file>
```

Zugriffsschlüssel hochladen

```
kesl-control [-D] --upload-temporary-device-access-key --path <access key>
```

Wobei gilt:

`--device-id <device ID>` ist die ID des gesperrten Geräts, auf das Sie zugreifen möchten.

`--access-duration <access duration>` ist der Zeitraum, für den Sie Zugriff auf das Gerät erhalten möchten (in Stunden). Mögliche Werte: 1 – 100.

`--path <path to access request file>` ist der Pfad zu dem Verzeichnis, in dem Sie die Zugriffsanforderungsdatei mit der Erweiterung .akey speichern möchten.

`--path <access key>` ist der Pfad zur Datei mit dem Zugriffsschlüssel für das Gerät (Datei mit der Erweiterung .acode).

Befehle zur Verwaltung der Programmkontrolle

Das Präfix -A gibt an, dass der Befehl zur Gruppe der Befehle zur Verwaltung der Programmkontrolle gehört.

Verwalten der Aufgabe „Inventarisierung“

```
Liste der auf dem Client-Gerät erkannten Programme anzeigen
```

```
kesl-control [-A] --get-app-list [--json]
```

Wobei gilt:

`--json` – Gibt Daten im JSON-Format aus.

Programmkategorien anzeigen

```
Liste der erstellten Kategorien der Programmkontrolle anzeigen
```

```
kesl-control [-A] --get-categories [--names <name of category 1> <name of category 2> ... <name of category N>] [-
-file <path to file>] [--json]
```

Wobei gilt:

`<category name 1> <category name 2> ... <category name N>` sind Kategorienamen. Wenn Sie Informationen mehrerer Kategorien anzeigen möchten, geben Sie die Kategorienamen durch ein Leerzeichen getrennt an.

`--file <path to file>` speichert oder exportiert Einstellungen in eine Konfigurationsdatei. Wenn diese Option nicht angegeben ist, wird das Ergebnis des Befehls in die Standardausgabe geschrieben.

`--json` – Gibt Daten im JSON-Format aus.

Verwalten von Programmkategorien

So erstellen Sie eine Programmkategorie:

1. Schreiben Sie die Liste der Programmkategorien in eine Konfigurationsdatei:

```
kesl-control --set-categories --file <path to file>
```

2. Fügen Sie Programmkategorien wie folgt hinzu:

```
[
   {
      "Exclude" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "GUID" : "<category ID>",
      "Include" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "Name" : "<category name 1>"
   },
 {
      "Exclude" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "GUID" : "<category ID>",
      "Include" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "Name" : "<category name 2>"
   }
]
```

Zur Angabe des Dateipfads in den Feldern `Exclude` und `Include` können Sie Masken verwenden.

3. Importieren Sie die Liste der Kategorien in das Programm:

```
kesl-control [-A] --set-categories [--names <category name 1> <category name 2> ... <name of category N>] --
file <path to file>
```

Liste der Kategorien der Programmkontrolle bearbeiten

```
kesl-control [-A] --set-categories [--names <category name 1> <category name 2> ... <name of category N>] --file
<path to file>
```

Wobei gilt:

`FilePath like <application>` ist ein vollständiger Pfad zur ausführbaren Datei des Programms.

`FileHash == <hash>` ist ein SHA256-Hash der ausführbaren Datei des Programms.

`<category ID>` ist eine eindeutige Kategorie-ID. Erforderliche Einstellung. Geben Sie `GUID` ohne Bindestriche ein.

`<category name 1> <category name 2> ... <category name N>` sind Kategorienamen. Erforderliche Einstellung.

Wenn Sie Informationen mehrerer Kategorien ändern möchten, geben Sie die Kategorienamen durch ein Leerzeichen getrennt an. Wenn Sie keinen Kategorienamen angeben, wird die Kategorie nicht erstellt oder aus der Liste der vorhandenen Kategorien gelöscht.

`--file <path to file>` speichert oder exportiert Einstellungen in eine JSON-Konfigurationsdatei.

Einstellungen der Programmkontrolle verwalten

Aktuelle Einstellungen der Programmkontrolle anzeigen

```
kesl-control --get-settings 21 [--file <path to file>] [--json]
```

Einstellungen der Programmkontrolle ändern

```
kesl-control --set-settings 21 [<setting>=<value>] [--file <path to file>] [--json]
```

Wobei gilt:

`<setting>=<value>` gibt eine Einstellung der Programmkontrolle und ihren Wert an.

`--file <path to file>` speichert oder exportiert Einstellungen in eine Konfigurationsdatei. Wenn diese Option nicht angegeben ist, wird das Ergebnis des Befehls in die Standardausgabe geschrieben.

`--json` – Gibt Daten im JSON-Format aus.

Einstellungen auf Standardwerte zurücksetzen

```
Eine Liste mit Programmkategorien und Regeln der Programmkontrolle löschen und die Standardeinstellungen wiederherstellen
```

```
kesl-control --set-settings 21 --set-to-default
```

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/dir/*/file*/` oder `/dir/file*/`.

Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.

Befehle zur Verwaltung der Web-Kontrolle

Verwalten der Einstellungen der Web-Kontrolle

```
Aktuelle Einstellungen der Web-Kontrolle anzeigen
```

```
kesl-control --get-settings 26 [--file <path to file>] [--json]
```

```
Einstellungen der Web-Kontrolle ändern
```

```
kesl-control --set-settings 26 [<setting>=<value>] [--file <path to file>] [--json]
```

Wobei gilt:

`<setting>=<value>` ist eine Einstellung der Web-Kontrolle und deren Wert. Sie können eine beliebige Anzahl von Einstellungen ändern.

`--file <path to file>` speichert oder exportiert Einstellungen in eine Konfigurationsdatei. Wenn diese Option nicht angegeben ist, wird das Ergebnis des Befehls in die Standardausgabe geschrieben.

`--json` – Gibt Daten im JSON-Format aus.

Einstellungen auf Standardwerte zurücksetzen

```
Konfigurierte Einstellungen löschen und Standardeinstellungen der Web-Kontrolle wiederherstellen
kesl-control --set-settings 26 --set-to-default
```

Schutz von Netzwerkverbindungen

Befehle zur Verwaltung blockierter Geräte

Das Präfix -H gibt an, dass der Befehl zur Gruppe der Befehle zur Verwaltung von Geräten gehört, die durch Schutz vor Verschlüsselung und Schutz vor Netzwerkbedrohungen blockiert wurden.

kesl-control --get-blocked-hosts

Mit diesem Befehl können Sie die Liste der blockierten Geräte in die Konsole ausgeben.

```
kesl-control [-H] --get-blocked-hosts
```

kesl-control --allow-hosts

Mit diesem Befehl können Sie gesperrte Geräte entsperren.

```
kesl-control [-H] --allow-hosts <address>
```

Wobei gilt:

`<address>` ist eine IP-Adresse eines Geräts oder Subnetzes (IPv4/IPv6, einschließlich Adressen in Kurzform). Sie können mehrere, durch Leerzeichen getrennte IP-Adressen von Geräten oder Subnetzen angeben.

Befehle zur Firewall-Verwaltung

Das Präfix -F gibt an, dass der Befehl zur Gruppe der Befehle zur Firewall-Verwaltung gehört.

Befehl kesl-control --add-rule

Mit diesem Befehl können Sie eine neue Netzwerkpaketregel hinzufügen.

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

Wobei gilt:

`--name <rule name>` ist der Name der Netzwerkpaketregel.

`--action <Allow|Block>` ist die Aktion, die für die in dieser Netzwerkpaketregel angegebenen Verbindungen ausgeführt werden soll.

`--protocol <protocol>` ist das Protokoll, für das die Netzwerkaktivität überwacht werden soll.

`--direction <direction>` ist die Richtung der überwachten Netzwerkaktivität.

`--remote <remote address>:<port>` ist die Netzwerkadresse des Remote-Geräts.

`--local <local address>:<port>` ist die Netzwerkadresse des Geräts, auf dem Kaspersky Endpoint Security installiert ist.

`--at <index>` ist die 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.

Netzwerkpaketregel anhand des Regelnamens löschen

```
kesl-control [-F] --del-rule --name <rule name>
```

Netzwerkpaketregel anhand der Regelnummer löschen

```
kesl-control [-F] --del-rule --index <index>
```

Wobei gilt:

`--name <rule name>` ist der Name der Netzwerkpaketregel.

`--index <index>` ist die Nummer der Regel in der Liste der Netzwerkpaketregeln.

Befehl kesl-control --move-rule

Mit diesem Befehl können Sie die Ausführungspriorität einer Netzwerkpaketregel ändern.

Priorität einer Netzwerkpaketregel anhand des Regelnamens ändern

```
kesl-control [-F] --move-rule --name <rule name> --at <index>
```

Priorität einer Netzwerkpaketregel anhand der Regelnummer ändern

```
kesl-control [-F] --move-rule --index <index> --at <index>
```

Wobei gilt:

`--name <rule name>` ist der Name der Netzwerkpaketregel.

`--index <index>` ist die aktuelle Nummer der Regel in der Liste der Netzwerkpaketregeln.

`--at <index>` ist die neue Nummer der Regel in der Liste der Netzwerkpaketregeln.

Befehl kesl-control --add-zone

Mit diesem Befehl können Sie eine Adresse zu einer Netzwerkzone hinzufügen.

```
kesl-control [-F] --add-zone --zone <zone> --address <address>
```

Wobei gilt:

`--zone <zone>` ist der vordefinierte Name der Netzwerkzone.

`--address <address>` ist die Netzwerkadresse oder das Subnetz.

Befehl kesl-control --del-zone

Mit diesem Befehl können Sie eine Adresse aus der Netzwerkzone löschen.

Adresse anhand einer Adresse oder eines Subnetzes aus einer Netzwerkzone entfernen

```
kesl-control [-F] --del-zone --zone <zone> --address <address>
```

Adresse anhand der Regelnummer aus einer Netzwerkzone entfernen

```
kesl-control [-F] --del-zone --zone <zone> --index <address index>
```

Wobei gilt:

`--zone <zone>` ist der vordefinierte Name der Netzwerkzone.

`--address <address>` ist die Netzwerkadresse oder das Subnetz.

`--index <address index>` ist die Nummer der Adresse in der Netzwerkzone.

kesl-control -F --query

Mit diesem Befehl können Sie die Firewall-Regeln anzeigen, die mithilfe von Kaspersky Endpoint Security erstellt wurden.

```
kesl-control -F --query
```

Schutz vor komplexen Bedrohungen und gezielten Angriffen

Befehle zur Verwaltung der Quarantäne

Das Präfix -Q zeigt an, dass der Befehl zur Gruppe von Befehlen gehört, die zur Verwaltung der Quarantäne verwendet werden.

kesl-control -Q --mass-remove

Mit diesem Befehl können Sie alle oder nur bestimmte Dateien aus der Quarantäne löschen.

```
Alle Dateien löschen
```

```
kesl-control -Q --mass-remove
```

```
Dateien löschen, die den Filterbedingungen entsprechen
```

```
kesl-control -Q --mass-remove --query "<filter conditions>"
```

Wobei gilt:

`<filter conditions>` gibt einen oder mehrere logische Ausdrücke im Format `<field> <comparison operator> '<value>'` an, die mit dem logischen Operator `and` kombiniert werden, um die Ergebnisse der Abfrage einzuschränken.

Befehl kesl-control --put

Dieser Befehl ist nur bei Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Optimum oder Kaspersky Managed Detection and Response verfügbar.

Mit diesem Befehl können Sie eine Datei in die Quarantäne verschieben.

```
kesl-control [-Q] --put <file path> [--md5] [--sha256] [--save-original-file]
```

Wobei gilt:

`<file path>` ist der Pfad zu der Datei, die Sie in die Quarantäne verschieben möchten.

`--md5` – MD5-Hash der Datei, die Sie in die Quarantäne verschieben möchten.

`--sha256` – Hash der Datei, die Sie in die Quarantäne verschieben möchten

`--save-original-file` – Originaldatei nicht löschen. Wenn Sie diesen Schlüssel nicht angeben, wird die Originaldatei gelöscht.

Befehl kesl-control -Q --query

Mit diesem Befehl können Sie Informationen über Quarantäne-Dateien anzeigen.

```
Informationen zu allen Quarantäne-Dateien anzeigen
```

```
kesl-control -Q --query [-n <number>] [--json]
```

```
Informationen zu Quarantäne-Dateien anzeigen, die den Filterbedingungen entsprechen
```

```
kesl-control -Q --query ["<filter conditions>"] [-n <number>]
```

Wobei gilt:

`<filter conditions>` gibt einen oder mehrere logische Ausdrücke im Format `<field> <comparison operator> '<value>'` an, die mit dem logischen Operator `and` kombiniert werden, um die Ergebnisse der Abfrage einzuschränken. Wenn Sie keine Filterbedingungen angeben, zeigt die App Informationen zu allen Quarantäne-Dateien an.

`<number>` ist die Anzahl der zuletzt in die Quarantäne verschobenen Dateien, die Sie anzeigen möchten. Wenn Sie den Schlüssel `-n` nicht angeben, werden die letzten 30 Dateien angezeigt. Um alle Dateien anzuzeigen, geben Sie den Wert 0 ein.

`--json` – Gibt Daten im JSON-Format aus.

Befehl kesl-control -Q --restore

Mit diesem Befehl können Sie eine Datei aus der Quarantäne wiederherstellen.

```
kesl-control -Q --restore <file ID> [--file <file path>]
```

Dabei gilt:

`<file ID>` ist die ID der Quarantäne-Datei.

`--file <file path>` ist der neue Name der Datei und der Pfad zu dem Verzeichnis, in dem die Datei gespeichert werden soll. Wenn Sie den Schlüssel `--file` nicht angeben, wird die Datei mit ihrem ursprünglichen Namen an ihrem ursprünglichen Speicherort wiederhergestellt. Wenn das Verzeichnis gelöscht wird oder der Benutzer keine Zugriffsrechte auf dieses Verzeichnis hat, legt die App die Datei im Verzeichnis /var/opt/kaspersky/kesl/common/restored/ ab. Sie können die Datei manuell aus diesem Verzeichnis in das gewünschte Verzeichnis verschieben.

Befehle zur Verwaltung der Komponente EDR Expert (on-premise)

Das Präfix -R gibt an, dass der Befehl zur Gruppe von Befehlen zur Verwaltung der Integrationseinstellungen mit Kaspersky Detection and Response-Lösungen gehört.

Befehl kesl-control --add-kataedr-server-certificate

Mit diesem Befehl können Sie dem KATA-Server, OSMP-Reaktionsserver oder OSMP-Telemetrieserver (abhängig vom Integrationsmodus) ein Zertifikat hinzufügen oder ein zuvor hinzugefügtes Zertifikat ersetzen.

```
kesl-control [-R] --add-kataedr-server-certificate <file> [--server-type <response|telemetry>]
```

Wobei gilt:

`<file>` ist der Pfad zur Datei, die das Serverzertifikat enthält.

Mit `--server-type <response|telemetry>` können Sie den Typ des Servers auswählen, für den Sie im Integrationsmodus von EDR Expert (on-premise) ein Zertifikat hinzufügen oder ersetzen möchten:

- `response` – Im Falle des OSMP-Reaktionsservers
- `telemetry` – Im Falle des OSMP-Telemetrieservers

Wenn Sie das Zertifikat eines KATA-Servers hinzufügen oder ersetzen möchten, geben Sie den Parameter `--server-type` nicht an.

Befehl kesl-control --remove-kataedr-server-certificate

Mit diesem Befehl können Sie das Zertifikat des KATA-Servers, OSMP-Reaktionsservers oder OSMP-Telemetrieservers (abhängig vom Integrationsmodus) löschen.

```
kesl-control [-R] --remove-kataedr-server-certificate [--server-type <response|telemetry>]
```

Wobei gilt:

Mit `--server-type <response|telemetry>` können Sie den Typ des Servers auswählen, für den Sie im Integrationsmodus von EDR Expert (on-premise) ein Zertifikat entfernen möchten:

- `response` – Im Falle des OSMP-Reaktionsservers
- `telemetry` – Im Falle des OSMP-Telemetrieservers

Wenn Sie das Zertifikat eines KATA-Servers löschen möchten, geben Sie den Parameter `--server-type` nicht an.

Befehl kesl-control --query-kataedr-server-certificate

Mit diesem Befehl können Sie Informationen über das Zertifikat des KATA-Servers, OSMP-Reaktionsservers oder OSMP-Telemetrieservers (abhängig vom Integrationsmodus) ausgeben.

```
kesl-control [-R] --query-kataedr-server-certificate [--server-type <response|telemetry>]
```

Wobei gilt:

Mit `--server-type <response|telemetry>` können Sie den Typ des Servers auswählen, für den Sie im Integrationsmodus von EDR Expert (on-premise) Zertifikatsinformationen anzeigen möchten:

- `response` – Im Falle des OSMP-Reaktionsservers
- `telemetry` – Im Falle des OSMP-Telemetrieservers

Wenn Sie Informationen über das Zertifikat eines KATA-Servers ausgeben möchten, geben Sie den Parameter `--server-type` nicht an.

Befehl kesl-control --add-kataedr-client-certificate

Mit diesem Befehl können Sie ein Client-Zertifikat, dass zum Schutz der Verbindung mit dem KATA-Server, OSMP-Reaktionsserver oder OSMP-Telemetrieserver (abhängig vom Integrationsmodus) verwendet wird, hinzufügen oder ein bereits hinzugefügtes ändern.

```
kesl-control [-R] --add-kataedr-client-certificate <file>  [--server-type <response|telemetry>]
```

Wobei gilt:

`<file>` ist der Pfad zum Crypto-Container (PFX-Archiv), der das Client-Zertifikat und den privaten Schlüssel enthält.

> Sie müssen das Kennwort für den Crypto-Container angeben. Andernfalls wird beim Klicken auf **Eingabe** ein `Certificate password is required and cannot be empty`-Fehler angezeigt.

Mit `--server-type <response|telemetry>` können Sie den Typ des Servers auswählen, für den Sie im Integrationsmodus von EDR Expert (on-premise) ein Client-Zertifikat hinzufügen möchten:

- `response` – Im Falle des OSMP-Reaktionsservers
- `telemetry` – Im Falle des OSMP-Telemetrieservers

Wenn Sie das Client-Zertifikat für die Verbindung mit einem KATA-Server hinzufügen oder ersetzen möchten, geben Sie den Parameter `--server-type` nicht an.

Befehl kesl-control --remove-kataedr-client-certificate

Mit diesem Befehl können Sie ein Client-Zertifikat, dass zum Schutz der Verbindung mit dem KATA-Server, OSMP-Reaktionsserver oder OSMP-Telemetrieserver (abhängig vom Integrationsmodus) verwendet wird, löschen.

```
kesl-control [-R] --remove-kataedr-client-certificate [--server-type <response|telemetry>]
```

Wobei gilt:

Mit `--server-type <response|telemetry>` können Sie den Typ des Servers auswählen, für den Sie im Integrationsmodus von EDR Expert (on-premise) ein Client-Zertifikat entfernen möchten:

- `response` – Im Falle des OSMP-Reaktionsservers
- `telemetry` – Im Falle des OSMP-Telemetrieservers

Wenn Sie das Client-Zertifikat für die Verbindung mit einem KATA-Server löschen möchten, geben Sie den Parameter `--server-type` nicht an.

Befehl kesl-control --query-kataedr-client-certificate

Mit diesem Befehl können Sie Informationen über ein Client-Zertifikat, das zum Schutz der Verbindung mit dem KATA-Server, OSMP-Reaktionsserver oder OSMP-Telemetrieserver (abhängig vom Integrationsmodus) verwendet wird, ausgeben.

```
kesl-control [-R] --query-kataedr-client-certificate [--server-type <response|telemetry>]
```

Wobei gilt:

Mit `--server-type <response|telemetry>` können Sie den Typ des Servers auswählen, für den Sie im Integrationsmodus von EDR Expert (on-premise) Informationen über ein Client-Zertifikat anzeigen möchten:

- `response` – Im Falle des OSMP-Reaktionsservers
- `telemetry` – Im Falle des OSMP-Telemetrieservers

Wenn Sie Informationen über das Client-Zertifikat für die Verbindung mit einem KATA-Server ausgeben möchten, geben Sie den Parameter `--server-type` nicht an.

Befehle zur Verwaltung der Komponente EDR Expert (cloud)

Das Präfix -R gibt an, dass der Befehl zur Gruppe von Befehlen zur Verwaltung der Integrationseinstellungen mit Kaspersky Detection and Response-Lösungen gehört.

kesl-control --query-cloudxdr-server-certificate

Mit diesem Befehl können Sie Informationen zu einem Zertifikat des OSMP-Servers für Bedrohungsreaktionen oder OSMP-Servers zur Erfassung von Telemetriedaten anzeigen.

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type <response|telemetry>
```

Wobei gilt:

`--server-type <response|telemetry>` ermöglicht die Auswahl des Servertyps, für den Sie im Integrationsmodus „EDR Expert (cloud)“ Zertifikatsinformationen anzeigen möchten:

- `response` – Im Falle des OSMP-Reaktionsservers
- `telemetry` – Im Falle des OSMP-Telemetrieservers

kesl-control --query-cloudxdr-client-certificate

Mit diesem Befehl können Sie Informationen zu einem zuvor hinzugefügten Client-Zertifikat anzeigen, das zum Schutz der Verbindung zum OSMP-Server für Bedrohungsreaktionen oder OSMP-Telemetrieserver verwendet wird.

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type <response|telemetry>
```

Wobei gilt:

`--server-type <response|telemetry>` ermöglicht die Auswahl des Servertyps, für den Sie im Integrationsmodus „EDR Expert (cloud)“ Informationen zu einem Client-Zertifikat anzeigen möchten:

- `response` – Im Falle des OSMP-Reaktionsservers
- `telemetry` – Im Falle des OSMP-Telemetrieservers

Befehle zur Verwaltung von NDR (KATA)

Das Präfix -R gibt an, dass der Befehl zur Gruppe von Befehlen zur Verwaltung der Integrationseinstellungen mit Kaspersky Detection and Response-Lösungen gehört.

Befehl kesl-control --add-katandr-server-certificate

Mit diesem Befehl können Sie ein zuvor hinzugefügtes Zertifikat des NDR-Servers hinzufügen oder ersetzen.

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

Wobei gilt:

`<file>` ist der Pfad zur Datei, die das Serverzertifikat enthält.

Befehl kesl-control --remove-katandr-server-certificate

Mit diesem Befehl wird ein NDR-Serverzertifikat entfernt.

```
kesl-control [-R] --remove-katandr-server-certificate
```

Befehl kesl-control --query-katandr-server-certificate

Mit diesem Befehl können Sie Informationen zum Zertifikat des NDR-Servers anzeigen.

```
kesl-control [-R] --query-katandr-server-certificate
```

Befehl kesl-control --add-katandr-client-certificate

Mit diesem Befehl können Sie ein zuvor hinzugefügtes Client-Zertifikat hinzufügen oder ersetzen, das zur Absicherung der Verbindung zum NDR-Server verwendet wird.

```
kesl-control [-R] --add-katandr-client-certificate <file>
```

Wobei gilt:

`<file>` ist der Pfad zum Crypto-Container (PFX-Archiv), der das Client-Zertifikat und den privaten Schlüssel enthält.

Sie müssen das Kennwort für den Crypto-Container angeben. Andernfalls wird beim Klicken auf **`Eingabe`** ein `Certificate password is required and cannot be empty`-Fehler angezeigt.

Befehl kesl-control --remove-katandr-client-certificate

Mit diesem Befehl können Sie das Client-Zertifikat löschen, das zur Absicherung der Verbindung zum NDR-Server verwendet wird.

```
kesl-control [-R] --remove-katandr-client-certificate
```

Befehl kesl-control --query-katandr-client-certificate

Mit diesem Befehl können Sie Informationen zum Client-Zertifikat ausgeben.

```
kesl-control [-R] --query-katandr-client-certificate
```

Befehle zur Verwaltung der Netzwerkisolation eines Geräts

Das Präfix -R gibt an, dass der Befehl zur Gruppe von Befehlen zur Verwaltung der Integrationseinstellungen mit Kaspersky Detection and Response-Lösungen gehört. Die Netzwerkisolation von Geräten wird bei einer Integration der angegebenen Detection and Response-Lösungen als Reaktionsmaßnahme beim Erkennen einer Bedrohung angewendet.

Befehl kesl-control --isolation-stat

Mit diesem Befehl können Sie den aktuellen Status der Netzwerkisolation in die Konsole ausgeben: aktiviert oder deaktiviert.

```
kesl-control [-R] --isolation-stat
```

Befehl kesl-control --isolation-off

Mit diesem Befehl können Sie die Netzwerkisolation des Geräts temporär deaktivieren.

```
kesl-control [-R] --isolation-off
```

Befehle zur Verwaltung der Integrationseinstellungen für KUMA

Das Präfix -M gibt an, dass der Befehl zur Befehlsgruppe für die Verwaltung der Einstellungen von Kaspersky Unified Monitoring and Analysis Platform gehört.

Befehl kesl-control --add-kuma-server-certificate

Mit diesem Befehl können Sie ein zuvor hinzugefügtes Zertifikat des KUMA-Servers hinzufügen oder ersetzen.

```
kesl-control [-M] --add-kuma-server-certificate <path to file>
```

Wobei gilt:

`<path to file>` ist der Pfad zu der Datei, die das Serverzertifikat im DER- oder PEM-Format enthält.

Befehl kesl-control --remove-kuma-server-certificate

Mit diesem Befehl können Sie das Zertifikat des KUMA-Servers löschen.

```
kesl-control [-M] --remove-kuma-server-certificate
```

Befehl kesl-control --query-kuma-server-certificate

Mit diesem Befehl können Sie Informationen zum Zertifikat des KUMA-Servers anzeigen.

```
kesl-control [-M] --query-kuma-server-certificate
```

Befehl kesl-control --add-kuma-client-certificate

Mit diesem Befehl können Sie ein zuvor hinzugefügtes Client-Zertifikat hinzufügen oder ersetzen, das zur Absicherung der Verbindung zum KUMA-Server verwendet wird.

```
kesl-control [-M] --add-kuma-client-certificate <path to file>
```

Wobei gilt:

`<path to file>` ist der Pfad zum Crypto-Container (PFX-Archiv), der das Client-Zertifikat und den privaten Schlüssel enthält.

> Sie müssen das Kennwort für den Crypto-Container angeben. Andernfalls wird beim Klicken auf **`Eingabe`** ein `Certificate password is required and cannot be empty`-Fehler angezeigt.

Befehl kesl-control --remove-kuma-client-certificate

Mit diesem Befehl können Sie das Client-Zertifikat löschen, das zur Absicherung der Verbindung zum KUMA-Server verwendet wird.

```
kesl-control [-M] --remove-kuma-client-certificate
```

Befehl kesl-control --query-kuma-client-certificate

Mit diesem Befehl können Sie Informationen zum Client-Zertifikat ausgeben.

```
kesl-control [-M] --query-kuma-client-certificate
```

Befehle zur Verwaltung der Integrationseinstellungen für Sandbox

Das Präfix -X gibt an, dass der Befehl zur Befehlsgruppe für die Verwaltung der Einstellungen für die Integration mit Sandbox gehört.

Befehl kesl-control --add-sandbox-server-certificate

Mit dem Befehl können Sie ein zuvor hinzugefügtes Zertifikat des Servers, der die Interaktion mit KATA Sandbox gewährleistet, hinzufügen oder ersetzen.

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

Wobei gilt:

`<file>` ist der Pfad zu der Datei, die das Serverzertifikat im DER- oder PEM-Format enthält.

Befehl kesl-control --remove-sandbox-server-certificate

Mit dem Befehl können Sie ein Zertifikat des Servers, der die Interaktion mit Sandbox gewährleistet, löschen.

```
kesl-control [-X] --remove-sandbox-server-certificate
```

Befehl kesl-control --query-sandbox-server-certificate

Mit dem Befehl können Sie für ein Zertifikat des Servers, der die Interaktion mit Sandbox gewährleistet, Informationen ausgaben.

```
kesl-control [-X] --query-sandbox-server-certificate
```

Befehl kesl-control --add-sandbox-client-certificate

Mit diesem Befehl können Sie ein zuvor hinzugefügtes Client-Zertifikat, das zur Absicherung der Verbindung mit dem Server, der die Interaktion mit Sandbox gewährleistet, verwendet wird, hinzufügen oder ersetzen.

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

Wobei gilt:

`<file>` ist der Pfad zum Crypto-Container (PFX-Archiv), der das Client-Zertifikat und den privaten Schlüssel enthält.

Sie müssen das Kennwort für den Crypto-Container angeben. Andernfalls wird beim Klicken auf **Eingabe** ein `Certificate password is required and cannot be empty`-Fehler angezeigt.

Befehl kesl-control --remove-sandbox-client-certificate

Mit diesem Befehl können Sie ein zuvor hinzugefügtes Client-Zertifikat löschen, das zur Absicherung der Verbindung mit dem Server, der die Interaktion mit Sandbox gewährleistet, verwendet wird.

```
kesl-control [-X] --remove-sandbox-client-certificate
```

Befehl kesl-control --query-sandbox-client-certificate

Mit diesem Befehl können Sie Informationen zum Client-Zertifikat ausgeben.

```
kesl-control [-X] --query-sandbox-client-certificate
```

Befehl kesl-control --sandbox

Mit diesem Befehl können Sie Dateien zur Untersuchung an Sandbox senden.

```
kesl-control [-X] --sandbox <path 1> <path 2>
```

Wobei gilt:

`<path>` ist der Pfad zu der Datei oder dem Verzeichnis, die bzw. das Sie untersuchen möchten. Sie können mehrere, durch Leerzeichen getrennte Pfade angeben.

Befehle zur Verwaltung der IOC-Untersuchung

Das Präfix `-T` gibt an, dass der Befehl zur Gruppe der Befehle zur Verwaltung von Programmeinstellungen und Aufgaben gehört.

Befehl kesl-control --scan-ioc

Der Befehl startet eine Suche nach Kompromittierungsindikatoren (IOC) auf dem Gerät.

```
kesl-control [-T] --scan-ioc --path <path to directory or file> [--process on|off] [--hint <regular expression>]
[--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives all|system|critical|custom] [--
excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

Wobei gilt:

`--path <path to directory or file>` ist der Pfad zu einer IOC-Datei oder zu einem Verzeichnis mit IOC-Dateien mit der Erweiterung .IOC oder .XML, der für die Durchführung der Untersuchung verwendet werden soll.

> Sie können mehrere, durch Leerzeichen getrennte Pfade angeben. Sie können auch beide Arten von Pfaden (Datei und Verzeichnis) angeben.

`--process` – Analyse der auf dem Gerät laufenden Prozesse aktivieren.

Mögliche Argumente:

- `on` – Analyse der auf dem Gerät ausgeführten Prozesse aktivieren (Standardwert).
- `off` – Analyse der auf dem Gerät ausgeführten Prozesse deaktivieren.

Wenn Sie den Parameter `--process` nicht angeben, führt die Anwendung nur dann eine Prozessanalyse durch, wenn die verwendete IOC-Datei Daten dieser Prozesse (`ProcessItem`) enthält.

`--hint <regular expression>` ist der reguläre Ausdruck, der dem vollständigen Pfad zur zu analysierenden Datei (`FileItem`) oder zur ausführbaren Datei des zu analysierenden Prozesses (`ProcessItem`) entspricht.

Für den regulären Ausdruck können folgende Elemente verwendet werden:

- Metazeichen: `.` `^` `$` `|`
- Zeichenklassen: `digit`, `alpha`, `lower`, `upper`, `cntrl`
- Quantifikatoren: `*` `+` `?` `{n}` `{n,}` `{n, m}`
- Negation: `[^a-c]`
- Geschützte Zeichen: `\a` `\e` `\f`, `\n` `\r` `\t` `\v` `\b`

`--arpentry` – Analyse von Einträgen in der ARP-Tabelle (`ArpEntryItem`) aktivieren.

Mögliche Argumente:

- `on` – Analyse von Einträge in der ARP-Tabelle aktivieren (Standardwert).
- `off` – Analyse von Einträgen in der ARP-Tabelle deaktivieren.

Wenn Sie den Parameter `--arpentry` nicht angeben, führt die Anwendung nur dann eine Analyse der ARP-Tabelle durch, wenn die verwendete IOC-Datei Daten dieser Tabelle (`ArpEntryItem`) enthält.

`--ports` – Analyse von Ports aktivieren, die geöffnet sind und Verbindungen empfangen können.

Mögliche Argumente:

- `on` – Analyse von geöffneten Ports und aktiven Verbindungen mit dem Gerät aktivieren (Standardwert).
- `off` – Analyse von geöffneten Ports und aktiven Verbindungen mit dem Gerät deaktivieren.

Wenn Sie den Parameter `--ports` nicht angeben, führt die Anwendung nur dann eine Portanalyse durch, wenn die verwendete IOC-Datei Daten dieser Ports (`PortItem`) enthält.

`--system` – Analyse der Systemumgebung aktivieren.

Mögliche Argumente:

- `on` – Analyse der Systemumgebung aktivieren (Standardwert).
- `off` – Analyse der Systemumgebung deaktivieren.

Wenn Sie den Parameter `--system` nicht angeben, führt die Anwendung nur dann eine Analyse der Systemumgebung durch, wenn die verwendete IOC-Datei Daten über die Systemumgebung (`SystemInfoItem`) enthält.

`--files` – Dateianalyse aktivieren.

Mögliche Argumente:

- `on` – Dateianalyse aktivieren (Standardwert).
- `off` – Dateianalyse deaktivieren.

Wenn Sie den Parameter `--files` nicht angeben, führt die Anwendung nur dann eine Dateianalyse durch, wenn die verwendete IOC-Datei Daten dieser Dateien (`FileItem`) enthält.

`--drives` – zu untersuchende Bereiche.

Mögliche Argumente:

- `all` – alle verfügbaren Dateibereiche untersuchen.
- `system` – Untersucht alle Dateien innerhalb des Stamm-Dateisystems.
- `critical` – Dateien in den Benutzer- und Systemverzeichnissen untersuchen (Standardwert).
- `custom` – nur die Dateien untersuchen, die sich in den von Ihnen angegebenen Bereichen befinden.

Wenn Sie den Parameter `--drives` nicht angeben, analysiert die Anwendung die Dateien in den Benutzer- und Systemverzeichnissen.

`--excludes <list of exclusions>` ist die Liste der von der Untersuchung ausgeschlossenen Pfade.

Die in diesem Parameter angegebenen Ausnahmen sind global und gelten unabhängig von der Art des Bereichs oder der Verzeichnisliste. Diese Ausnahmen haben Vorrang vor anderen Befehlszeilenoptionen, einschließlich `--hint` und `--scope`.

> Ausschlüsse werden als Pfade angegeben, dürfen jedoch keine rekursiven Elemente oder Masken-Symbole (wie `*`) enthalten.

Wenn Sie den Parameter `--excludes` nicht angeben, wird die Untersuchung ohne Ausschlüsse durchgeführt.

Sie können mehrere, durch Leerzeichen getrennte Ausschlüsse angeben.

`--scope <list of directories>` ist die Liste der zusätzlichen Verzeichnisse, die untersucht werden sollen.

> Diese Option ist erforderlich, wenn Sie das Argument `--drives` für die Option `custom` angegeben haben.

`--action` – Aktion, die bei Erkennung eines Kompromittierungsindikators ausgeführt werden soll.

Mögliche Argumente:

- `Skip` – die Anwendung führt keine Aktionen mit dem erkannten Objekt aus, aber Informationen darüber werden in den Ergebnissen der Aufgabenausführung gespeichert (Standardwert).
- `QuarantineFile` – die Anwendung verschiebt das erkannte Objekt in die Quarantäne.
- `IsolateHost` – die Anwendung isoliert das Gerät, auf dem das Objekt erkannt wurde, vom Netzwerk.
- `ScanCriticalAreas` – die Anwendung führt eine Untersuchung wichtiger Bereiche durch.

Von Kaspersky Endpoint Security untersuchte wichtige Bereiche

- /lib/systemd
- /lib/udev
- /lib/dbus-1.0
- /usr/local/lib/systemd/user
- /usr/share/dbus-1
- /usr/share/gdm/autostart
- /usr/share/gnome/autostart
- /var/spool/at
- /var/spool/at/spool
- /var/spool/anacron
- /var/spool/cron
- /boot
- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64

- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

Sie können mehrere, durch Leerzeichen getrennte Aktionen angeben.

Wenn Sie das Argument `Skip` angegeben haben, müssen Sie keine weiteren Argumente hinzufügen. Das Argument `Skip` kann nur alleinstehend verwendet werden.

kesl-control --get-response-task-list

Dieser Befehl zeigt Informationen zu laufenden *IOC-Untersuchung*-Aufgaben auf dem Gerät an.

```
kesl-control [-T] --get-response-task-list
```

Daraufhin zeigt die Anwendung Informationen zu laufenden Aufgaben in folgender Form an:

Aufgaben-ID: <Aufgaben-ID>

Reaktion: locScan

Erstellungsdatum: <Datum und Uhrzeit der Aufgabenerstellung>

Aufgabe starten: <Zeitplan für den Aufgabenstart>

Status: <Aufgabenstatus>

Kaspersky Endpoint Security aktualisiert bei jeder Synchronisierung mit dem Server Informationen zu laufenden *IOC-Untersuchung*-Aufgaben. Sie können den Synchronisierungszeitraum in den Einstellungen der Integration mit der Kaspersky Detection and Response-Lösung konfigurieren (`SynchronizationPeriod`). Standardmäßig synchronisiert sich die Anwendung alle 5 Minuten mit dem Server.

kesl-control --delete-response-task <task ID>

Dieser Befehl löscht die *IOC-Untersuchung*-Aufgabe anhand der ID. Die Anwendung löscht die Aufgabe lokal auf dem Computer. Wenn Sie die Aufgabe nicht in der Web Console oder in der OSMP Console gelöscht haben, stellt die Anwendung diese Aufgabe bei der nächsten Synchronisierung mit dem Server wieder her.

```
kesl-control [-T] --delete-response-task-list <task ID>
```

Programmbefehle im Light Agent-Modus

Das Präfix -V gibt an, dass der Befehl zur Gruppe der Befehle von Kaspersky Endpoint Security gehört, die im Light Agent-Modus verwendet werden.

Diese Befehle können nur ausgeführt werden, wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird.

kesl-control --ksvla-info

Dieser Befehl gibt Informationen zur Verwendung des Programms im Light Agent-Modus aus.

```
kesl-control --ksvla-info
```

kesl-control --viis-info

Dieser Befehl gibt Informationen über die Verbindung des Programms im Light Agent-Modus mit dem Integrationsserver aus.

```
kesl-control --viis-info
```

kesl-control --svm-info

Dieser Befehl gibt Informationen über die Verbindung des Programms im Light Agent-Modus mit der SVM aus.

```
kesl-control --svm-info
```

Befehlszeilenoptionen des Programms

Update-Aufgabe

In der folgenden Tabelle werden alle verfügbaren Werte und Standardwerte aller Einstellungen beschrieben, die Sie für die Aufgabe `Update` angeben können.

Einstellungen der Update-Aufgabe

Einstellung	Description	Werte
`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 Anwendung auf eine andere angegebene Update-Quelle zu.	Sie können nur ganze Zahlen zwischen 0 und 120 angeben. Standardwert: 10.
`ApplicationUpdateMode`	Modus für das Herunterladen und Installieren automatischer installierbarer Anwendungsupdates (Autopatches)	`Disabled` – Keine Autopatches herunterladen und installieren. `DownloadOnly` (Standardwert) – Autopatches automatisch herunterladen, aber nicht installieren. `DownloadAndInstall` – Autopatches automatisch herunterladen und installieren. Nach der Installation eines Autopatches wird die Anwendung automatisch neu gestartet.
Der Abschnitt **[Sources.item_#]** enthält die folgenden Einstellungen:		
`Enabled`	Verwendung der in der Einstellung `SourceType` angegebenen Update-Quelle. Um die Aufgabe abzuschließen, müssen Sie mindestens eine Update-Quelle aktivieren.	`Yes` (Standardwert) – Die Anwendung verwendet die Update-Quelle. `No` – Die Anwendung verwendet Update-Quelle nicht.
`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 Updates von dem im lokalen Netzwerk installierten Administrationsserver auf das geschützte Gerät herunter. Sie können diese Update-Quelle auswählen, wenn Sie Kaspersky Security Center für die zentrale Verwaltung des Schutzes der Geräte in Ihren Unternehmen benutzen. `Custom`. Die App lädt Updates aus einer benutzerdefinierten Quelle herunter, die in der Einstellung `URL` angegeben ist. 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.
`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 Anwendungsdatenbanken auf dem geschützten Gerät.

Geräteschutz vor Bedrohungen

Aufgabe zum Schutz vor bedrohlichen Dateien

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.

Die folgende Tabelle beschreibt alle möglichen Werte und Standardwerte aller Einstellungen, die Sie für die Aufgabe zum Schutz vor bedrohlichen Dateien festlegen können.

Einstellungen der Aufgabe zum Schutz vor bedrohlichen Dateien

Parameter	Description	Werte
`ScanArchived`	Aktiviert die Untersuchung von Archiven (einschließlich selbstentpackender sfx-Archive). Die Anwendung 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 Anwendungsdatenbanken ab. Es wird nicht empfohlen, diese Option zu aktivieren. Das Untersuchen von Archiven verringert die Leistung, da der Zugriff auf die Archivdatei wird blockiert, bevor die Datei in ein temporäres Verzeichnis entpackt und untersucht wird.	`Yes` – Archive untersuchen. Wenn für den Parameter `ActionOnThreat` der Wert `DisinfectDeleteIfNotPossible` angegeben und eine Desinfizierung nicht möglich ist, löscht die Anwendung 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 nur selbstentpackenden Archiven (Archiven, zu deren Bestandteilen ein ausführbares Dekompressionsmodul gehört).	`Yes` – Selbstentpackende Archive 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 Nur-Text-Format untersuchen. `No` (Standardwert) – E-Mail-Nachrichten im Textformat nicht untersuchen.

Parameter	Description	Werte
`SkipPlainTextFiles`	Dateien im Textformat vorübergehend von der Untersuchung ausschließen. Mit diesem Parameter können Sie die Untersuchung von Programmprotokollen optimieren. Dieser Parameter wird angewendet, wenn Sie den Mechanismus zum Abfangen von Systemereignissen auf Basis der fanotify-Technologie verwenden. Bei Verwendung des aktualisierbaren Kernel-Moduls wird die Untersuchung durch die Zwischenspeicherung von Untersuchungsergebnissen optimiert.	`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 Textformat werden untersucht.
`SkipDatabaseJournals`	Schließt Protokolldateien von Datenbanken vorübergehend von der Untersuchung aus. Mit diesem Parameter können Sie die Untersuchung von Datenbankprotokollen optimieren. Dieser Parameter wird angewendet, wenn Sie den Mechanismus zum Abfangen von Systemereignissen auf Basis der fanotify-Technologie verwenden. Bei Verwendung des aktualisierbaren Kernel-Moduls wird die Untersuchung durch die Zwischenspeicherung von Untersuchungsergebnissen optimiert.	`Yes` – Datenbankprotokolldateien nicht untersuchen, wenn diese Dateien vom selben Prozess innerhalb von 10 Minuten nach der letzten Untersuchung wiederverwendet werden. `No` (Standardwert) – Datenbankprotokolldateien untersuchen.
`SizeLimit`	Maximale Größe des zu untersuchenden Objekts (in Megabyte). Wenn die Größe des zu untersuchenden Objekts den angegebenen Wert überschreitet, überspringt die Anwendung das Objekt während der Untersuchung.	0 – 999999 0 – Die Anwendung untersucht Objekte beliebiger Größe. Standardwert: 0.
`TimeLimit`	Maximale Untersuchungsdauer (in Sekunden) eines Objekts. Die Anwendung 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: 60.
`ActionOnThreat`	Auswahl der Aktion, welche die Anwendung für infizierte Objekte ausführen soll.	`DisinfectDeleteIfNotPossible` (Desinfizieren. Entfernen, wenn Desinfektion fehlschlägt) – Die Anwendung versucht, das infizierte Objekt zu desinfizieren und speichert eine Kopie des Objekts im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), löscht die Anwendung das Objekt. `DisinfectBlockIfNotPossible` (Desinfizieren. Blockieren, wenn Desinfektion fehlschlägt) – Die Anwendung versucht, das infizierte Objekt zu desinfizieren und speichert eine Kopie des Objekts im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), blockiert die Anwendung den Zugriff auf das Objekt. `Block` (blockieren) – die Anwendung blockiert den Zugriff auf das infizierte Objekt. Der Standardwert ist: `DisinfectDeleteIfNotPossible`.

Parameter	Description	Werte
`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, von Untersuchungen ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht von der Untersuchung ausschließen.

`ExcludeMasks.item_#`	Ausnahme 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, aus der Untersuchung.	`Yes` – Objekte, welche die in der Einstellung `ExcludeThreats.item_#` angegebenen Bedrohungen enthalten, von der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die Bedrohungen enthalten, die in der Einstellung `ExcludeThreats.item_#` angegeben sind, nicht von der Untersuchung 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 verwenden, um Informationen über Ihr Netzwerk zu erhalten. Damit es von der Anwendung 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 Anwendung 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 Anwendung 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 Anwendung untersucht wurde.	`Yes` – Informationen über untersuchte Objekte in Archiven 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.

Parameter	Description	Werte
`UseAnalyzer`	Aktiviert die heuristische Analyse. Mithilfe der heuristischen Analyse kann die App Bedrohungen bereits erkennen, bevor sie den Virenanalysten bekannt sind. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`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. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`Light` – Oberflächlichste Untersuchung mit minimaler Belastung des Systems. `Medium` – Eine mittlere Stufe der heuristischen Analyse bei ausgewogener Systemauslastung. `Deep` – Die gründlichste Untersuchung bei maximaler Systemauslastung. `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:		
`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.	Der Standardwert ist: `All objects`. **Beispiel** `AreaDesc="Scanning of email databases"`
`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 Anwendung nur Dateien, die mit Masken im Shell-Format angegeben wurden. Wenn die Einstellung nicht angegeben wurde, untersucht die Anwendung alle Objekte im Untersuchungsbereich. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: `*` (alle Objekte untersuchen) **Beispiel** `AreaMask_item_<item number>=*doc`

Parameter	Description	Werte
`Path`	Pfad zum Verzeichnis mit untersuchten Objekten.	`<path to local folder>` – Objekte in dem angegebenen Verzeichnis untersuchen. Bei der Angabe des Pfades können Sie Masken und Tags 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. `<file system type>` – Alle Ressourcen des angegebenen Dateisystemgeräts 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.	`<path to local folder>` – Objekte im angegebenen Verzeichnis (einschließlich Unterverzeichnissen) von Untersuchungen ausschließen. Bei der Angabe des Pfades können Sie Masken und Tags verwenden. `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. `<file system>` – Alle Ressourcen des angegebenen Dateisystemgeräts von der Untersuchung ausschließen.
Der Abschnitt **[ExcludedForProgram.item_#]** enthält die folgenden Einstellungen:		
`ProgramPath`	Pfad des auszuschließenden Prozesses. Wenn für das Abfangen von Systemereignissen das aktualisierbare Kernel-Modul verwendet wird, wird der angegebene Prozess in allen Namensräumen vom Abfangen ausgeschlossen.	`<path to process>` — Objekte im angegebenen Verzeichnis von der Untersuchung ausschließen.

Parameter	Description	Werte
`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.
`AreaDesc`	Beschreibung des Ausschlussbereichs von Prozessen.	Der Standardwert ist: `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.	`<path to local folder>` — Objekte im angegebenen Verzeichnis von der Untersuchung ausschließen. Bei der Angabe des Pfades können Masken verwendet werden. `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. `<file system type>` – Alle Ressourcen des angegebenen Dateisystemgeräts von der Untersuchung ausschließen.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

So verwenden Sie Tags

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Wobei gilt:

`<id>` ist die Container-ID.

`<name>` ist ein Containername

`<path to local directory>` ist der Pfad zum lokalen Verzeichnis.

Sie können auch eindeutige Kombinationen von Tags verwenden: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` und `[image-name:<name>]/path to local directory>`.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispielsweise:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

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 eine Konfigurationsdatei aus:

   ```
   kesl-control --get-settings 1 --file <full path to the configuration file> [--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: `Yes` oder `No`).
   - `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 folgenden Befehl aus:

   ```
   kesl-control --set-settings 1 --file <full path to the configuration file> [--json]
   ```

   Geben Sie den Schalter `--json` an, wenn Sie Einstellungen aus einer Konfigurationsdatei im JSON-Format importieren. Wenn Sie keinen Schalter angeben, versucht die Anwendung, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

Die Anwendung untersucht keine Dateien in Netzwerkverzeichnissen. Allerdings werden der Befehl `cp` (für das oben genannte Beispiel) und lokale Dateien untersucht.

Schadsoftware-Untersuchung

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 oder fortsetzen und den Zeitplan der Aufgabe konfigurieren. Sie können die Einstellungen für die Untersuchung konfigurieren, indem Sie die Einstellungen für diese Aufgabe ändern.

- Mithilfe von benutzerdefinierten Aufgaben zur Schadsoftware-Untersuchung (Aufgaben vom Typ `ODS`). Sie können Benutzeraufgaben manuell starten, beenden, anhalten oder fortsetzen und den Zeitplan für den Aufgabenstart konfigurieren.

Sie können eine *benutzerdefinierte Untersuchung* der angegebenen Dateien und Verzeichnisse mit dem folgenden Befehl ausführen:

```
kesl-control --scan-file
```

Aufgabe zur Schadsoftware-Untersuchung

Die Tabelle beschreibt alle möglichen Werte sowie die Standardwerte aller Einstellungen, die Sie für die Aufgabe „Schadsoftware-Untersuchung“ (`Scan_My_Computer`) angeben können.

Untersuchungsparameter der Aufgabe zur Schadsoftware-Untersuchung

Einstellung	Description	Werte
`ScanFiles`	Aktiviert die Untersuchung von Dateien.	`Yes` (Standardwert) – Dateien untersuchen. `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) – Prozessspeicher und Kernelspeicher untersuchen. `No` – Prozessspeicher und Kernelspeicher nicht untersuchen.
`ScanStartupObjects`	Aktiviert die Untersuchung der Autostart-Objekte.	`Yes` (Standardwert) – Autostart-Objekte untersuchen. `No` – Autostart-Objekte nicht untersuchen.
`ScanArchived`	Aktiviert die Untersuchung von Archiven (einschließlich selbstentpackender sfx-Archive). Die Anwendung 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 untersuchen. Wenn für den Parameter `ActionOnThreat` der Wert `DisinfectDeleteIfNotPossible` angegeben und eine Desinfizierung nicht möglich ist, löscht die Anwendung 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.

Einstellung	Description	Werte
`ScanPlainMail`	Aktiviert die Untersuchung von E-Mail-Nachrichten im Textformat (plain text).	`Yes` – E-Mail-Nachrichten im Nur-Text-Format untersuchen. `No` (Standardwert) – E-Mail-Nachrichten im 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.
`QueueScanTasks`	Geplante Untersuchungsaufgaben verzögern, wenn eine zuvor gestartete geplante Untersuchung noch ausgeführt wird. Kaspersky Endpoint Security reiht geplante Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Eine Untersuchungsaufgabe soll beispielsweise um 18:00 Uhr und um 20:00 Uhr ausgeführt werden. Die für 20:00 Uhr geplante Untersuchungsaufgabe wird verzögert, wenn die Untersuchung um 18:00 Uhr noch ausgeführt wird. Die verzögerte Aufgabe wird ausgeführt, nachdem die Aufgabe um 18:00 Uhr beendet wurde.	`Yes`, um geplante Untersuchungsaufgaben in die Warteschlange einzureihen, wenn die aktuelle Untersuchung noch ausgeführt wird. `No` (Standardwert), um geplante Untersuchungsaufgaben auch dann auszuführen, wenn die aktuelle Untersuchung noch ausgeführt wird.
`ActionOnThreat`	Auswahl der Aktion, welche die Anwendung für infizierte Objekte ausführen soll.	`DisinfectDeleteIfNotPossible` (Desinfizieren. Entfernen, wenn Desinfektion fehlschlägt) – Die Anwendung versucht, das infizierte Objekt zu desinfizieren und speichert eine Kopie des Objekts im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), löscht die Anwendung das Objekt. `DisinfectInformIfNotPossible` (Desinfizieren. Informieren, wenn Desinfektion fehlschlägt) – Die Anwendung versucht, das infizierte Objekt zu desinfizieren und speichert eine Kopie des Objekts im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), speichert die Anwendung Informationen darüber im Protokoll. `Inform` (Informieren) – Die Anwendung unternimmt keinen Versuch, das infizierte Objekt zu desinfizieren oder zu löschen. Informationen über das infizierte Objekt werden im Protokoll gespeichert. Der Standardwert ist: `DisinfectDeleteIfNotPossible`.
`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, von Untersuchungen ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht von der Untersuchung ausschließen.

`ExcludeMasks.item_#`	Ausnahme 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 die Werte 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.*`

Einstellung	Description	Werte
`UseExcludeThreats`	Aktiviert den Ausschluss von Objekten mit Bedrohungen, die durch die Einstellung `ExcludeThreats.item_#` festgelegt sind, aus der Untersuchung.	`Yes` – Objekte, welche die in der Einstellung `ExcludeThreats.item_#` angegebenen Bedrohungen enthalten, von der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die Bedrohungen enthalten, die in der Einstellung `ExcludeThreats.item_#` angegeben sind, nicht von der Untersuchung 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 verwenden, um Informationen über Ihr Netzwerk zu erhalten. 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 Anwendung 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` – Globale Ausnahmen nicht verwenden.
`UseOASExclusions`	Aktivieren der Verwendung der Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der Untersuchung.	`Yes` (Standardwert) – Ausschlüsse aus dem Schutz vor bedrohlichen Dateien verwenden. `No` – Ausnahmen für den Schutz vor bedrohlichen Dateien nicht 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 untersuchte Objekte in Archiven 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. 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.

Einstellung	Description	Werte
`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 mit minimaler Belastung des Systems. `Medium` – Eine mittlere Stufe der heuristischen Analyse bei ausgewogener Systemauslastung. `Deep` – Die gründlichste Untersuchung bei maximaler Systemauslastung. `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 Gerätenamen. Die App untersucht die Bootsektoren dieser Geräte. Der Einstellungswert darf nicht leer sein. Um die Aufgabe auszuführen, müssen Sie mindestens eine Maske für Gerätenamen angeben.	`AllObjects` – Untersuchung der Bootsektoren aller Geräte. `<device name mask>` – Bootsektoren der Geräte untersuchen, deren Namen der angegebenen Maske entsprechen. Standardwert: `/**` (beliebiger Zeichensatz im Gerätenamen, einschließlich des Zeichens `/`)
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.	Der Standardwert ist: `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 Anwendung 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_0000=*doc`
`Path`	Pfad zum Verzeichnis mit untersuchten Objekten.	`<path to local directory>` – Objekte in dem 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. `<file system type>` – Alle Ressourcen des angegebenen Dateisystemgeräts untersuchen.
Der Abschnitt **[ExcludedFromScanScope.item_#]** enthält die folgenden Parameter:		

Einstellung	Description	Werte
`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 Anwendung 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 ausschließen)
`Path`	Pfad zum Verzeichnis mit ausgeschlossenen Objekten.	`<path to local directory>` – Objekte im angegebenen Verzeichnis (einschließlich Unterverzeichnissen) von Untersuchungen ausschließen. Bei der Angabe des Pfades können Masken verwendet werden. 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/`. Der Pfad `/` ist standardmäßig angegeben. Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus. `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. `<file system type>` – Alle Ressourcen des angegebenen Dateisystemgeräts von der Untersuchung ausschließen. Remote-Verzeichnisse werden nur dann von der Untersuchung durch die Anwendung ausgeschlossen, wenn sie bereits vor dem Aufgabenstart eingebunden wurden. Remote-Verzeichnisse, die erst nach dem Aufgabenstart eingebunden wurden, werden von der Untersuchung nicht ausgeschlossen.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Aufgabe zur benutzerdefinierten Untersuchung

Die Tabelle beschreibt alle verfügbaren Werte und Standardwerte aller Einstellungen, die Sie für die Aufgabe zur benutzerdefinierten Untersuchung (`Scan_File`) angeben können.

Einstellungen der Aufgabe zur benutzerdefinierten Untersuchung

Einstellung	Description	Werte
`ScanFiles`	Aktiviert die Untersuchung von Dateien.	`Yes` (Standardwert) – Dateien untersuchen. `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` – Prozessspeicher und Kernelspeicher untersuchen. `No` (Standardwert) – Prozess-Speicher und 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 Anwendung 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 untersuchen. Wenn für den Parameter `ActionOnThreat` der Wert `DisinfectDeleteIfNotPossible` angegeben und eine Desinfizierung nicht möglich ist, löscht die Anwendung 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 Nur-Text-Format untersuchen. `No` (Standardwert) – E-Mail-Nachrichten im 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.

Einstellung	Description	Werte
`QueueScanTasks`	Geplante Untersuchungsaufgaben verzögern, wenn eine zuvor gestartete geplante Untersuchung noch ausgeführt wird. Kaspersky Endpoint Security reiht geplante Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Eine Untersuchungsaufgabe soll beispielsweise um 18:00 Uhr und um 20:00 Uhr ausgeführt werden. Die für 20:00 Uhr geplante Untersuchungsaufgabe wird verzögert, wenn die Untersuchung um 18:00 Uhr noch ausgeführt wird. Die verzögerte Aufgabe wird ausgeführt, nachdem die Aufgabe um 18:00 Uhr beendet wurde.	`Yes`, um geplante Untersuchungsaufgaben in die Warteschlange einzureihen, wenn die aktuelle Untersuchung noch ausgeführt wird. `No` (Standardwert), um geplante Untersuchungsaufgaben auch dann auszuführen, wenn die aktuelle Untersuchung noch ausgeführt wird.
`ActionOnThreat`	Auswahl der Aktion, welche die Anwendung für infizierte Objekte ausführen soll.	`DisinfectDeleteIfNotPossible` (Desinfizieren. Entfernen, wenn Desinfektion fehlschlägt) – Die Anwendung versucht, das infizierte Objekt zu desinfizieren und speichert eine Kopie des Objekts im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), löscht die Anwendung das Objekt. `DisinfectInformIfNotPossible` (Desinfizieren. Informieren, wenn Desinfektion fehlschlägt) – Die Anwendung versucht, das infizierte Objekt zu desinfizieren und speichert eine Kopie des Objekts im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), speichert die Anwendung Informationen darüber im Protokoll. `Inform` (Informieren) – Die Anwendung unternimmt keinen Versuch, das infizierte Objekt zu desinfizieren oder zu löschen. Informationen über das infizierte Objekt werden im Protokoll gespeichert. Der Standardwert ist: `DisinfectDeleteIfNotPossible`.
`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, von Untersuchungen ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht von der Untersuchung ausschließen.

`ExcludeMasks.item_#`	Ausnahme 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, aus der Untersuchung.	`Yes` – Objekte, welche die in der Einstellung `ExcludeThreats.item_#` angegebenen Bedrohungen enthalten, von der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die Bedrohungen enthalten, die in der Einstellung `ExcludeThreats.item_#` angegeben sind, nicht von der Untersuchung ausschließen.

Einstellung	Description	Werte

`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 verwenden, um Informationen über Ihr Netzwerk zu erhalten. 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 Anwendung 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), um globale Ausnahmen zu verwenden. `No` – Globale Ausnahmen nicht verwenden.
`UseOASExclusions`	Aktivieren der Verwendung der Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der Untersuchung.	`Yes` (Standardwert), um Ausnahmen des Schutzes vor bedrohlichen Dateien zu verwenden. `No` – Ausnahmen für den Schutz vor bedrohlichen Dateien nicht 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), um Informationen zu nicht infizierten Objekten nicht im Protokoll zu 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 untersuchte Objekte in Archiven im Protokoll speichern. `No` (Standardwert), um Informationen über untersuchte Objekte in Archiven nicht im Protokoll zu 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), um Informationen zu nicht verarbeiteten Objekten nicht im Protokoll zu speichern.
`UseAnalyzer`	Aktiviert die heuristische Analyse. Mithilfe der heuristischen Analyse kann die App Bedrohungen bereits erkennen, bevor sie den Virenanalysten bekannt sind.	`Yes` (Standardwert), um die heuristische Analyse zu aktivieren. `No` – Heuristische Analyse deaktivieren.

Einstellung	Description	Werte
`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 mit minimaler Belastung des Systems. `Medium` – Eine mittlere Stufe der heuristischen Analyse bei ausgewogener Systemauslastung. `Deep` – Die gründlichste Untersuchung bei maximaler Systemauslastung. `Recommended` (Standardwert) – Der empfohlene Wert.
`UseIChecker`	Aktiviert die Nutzung der iChecker-Technologie.	`Yes` (Standardwert), um die Nutzung der iChecker-Technologie zu aktivieren. `No` – Nutzung der iChecker-Technologie deaktivieren.
`DeviceNameMasks.item_#`	Liste mit Gerätenamen. Die App untersucht die Bootsektoren dieser Geräte. Der Einstellungswert darf nicht leer sein. Um die Aufgabe auszuführen, müssen Sie mindestens eine Maske für Gerätenamen angeben.	`AllObjects` – Untersuchung der Bootsektoren aller Geräte. `<device name mask>` – Bootsektoren der Geräte untersuchen, deren Namen der angegebenen Maske entsprechen. Standardwert: `/**` (beliebiger Zeichensatz im Gerätenamen, einschließlich des Zeichens `/`)

Aufgabe zur Untersuchung wichtiger Bereiche

Die folgende Tabelle beschreibt alle verfügbaren Werte und Standardwerte aller Einstellungen, die Sie für die Aufgabe „Untersuchung wichtiger Bereiche“ (`Critical_Areas_Scan`) angeben können.

Einstellungen der Aufgabe zur Untersuchung wichtiger Bereiche

Einstellung	Description	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) – Prozessspeicher und Kernelspeicher untersuchen. `No` – Prozessspeicher und Kernelspeicher nicht untersuchen.
`ScanStartupObjects`	Aktiviert die Untersuchung der Autostart-Objekte.	`Yes` (Standardwert) – Autostart-Objekte untersuchen. `No` – Autostart-Objekte nicht untersuchen.
`ScanArchived`	Aktiviert die Untersuchung von Archiven (einschließlich selbstentpackender sfx-Archive). Die Anwendung 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 untersuchen. Wenn für den Parameter `ActionOnThreat` der Wert `DisinfectDeleteIfNotPossible` angegeben und eine Desinfizierung nicht möglich ist, löscht die Anwendung 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.

Einstellung	Description	Werte
`ScanPlainMail`	Aktiviert die Untersuchung von E-Mail-Nachrichten im Textformat (plain text).	`Yes` – E-Mail-Nachrichten im Nur-Text-Format untersuchen. `No` (Standardwert) – E-Mail-Nachrichten im 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.
`QueueScanTasks`	Geplante Untersuchungsaufgaben verzögern, wenn eine zuvor gestartete geplante Untersuchung noch ausgeführt wird. Kaspersky Endpoint Security reiht geplante Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Eine Untersuchungsaufgabe soll beispielsweise um 18:00 Uhr und um 20:00 Uhr ausgeführt werden. Die für 20:00 Uhr geplante Untersuchungsaufgabe wird verzögert, wenn die Untersuchung um 18:00 Uhr noch ausgeführt wird. Die verzögerte Aufgabe wird ausgeführt, nachdem die Aufgabe um 18:00 Uhr beendet wurde.	`Yes`, um geplante Untersuchungsaufgaben in die Warteschlange einzureihen, wenn die aktuelle Untersuchung noch ausgeführt wird. `No` (Standardwert), um geplante Untersuchungsaufgaben auch dann auszuführen, wenn die aktuelle Untersuchung noch ausgeführt wird.
`ActionOnThreat`	Auswahl der Aktion, welche die Anwendung für infizierte Objekte ausführen soll.	`DisinfectDeleteIfNotPossible` (Desinfizieren. Entfernen, wenn Desinfektion fehlschlägt) – Die Anwendung versucht, das infizierte Objekt zu desinfizieren und speichert eine Kopie des Objekts im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), löscht die Anwendung das Objekt. `DisinfectInformIfNotPossible` (Desinfizieren. Informieren, wenn Desinfektion fehlschlägt) – Die Anwendung versucht, das infizierte Objekt zu desinfizieren und speichert eine Kopie des Objekts im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), speichert die Anwendung Informationen darüber im Protokoll. `Inform` (Informieren) – Die Anwendung unternimmt keinen Versuch, das infizierte Objekt zu desinfizieren oder zu löschen. Informationen über das infizierte Objekt werden im Protokoll gespeichert. Der Standardwert ist: `DisinfectDeleteIfNotPossible`.
`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, von Untersuchungen ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht von der Untersuchung ausschließen.

`ExcludeMasks.item_#`	Ausnahme 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 die Werte 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.*`

Einstellung	Description	Werte
`UseExcludeThreats`	Aktiviert den Ausschluss von Objekten mit Bedrohungen, die durch die Einstellung `ExcludeThreats.item_#` festgelegt sind, aus der Untersuchung.	`Yes` – Objekte, welche die in der Einstellung `ExcludeThreats.item_#` angegebenen Bedrohungen enthalten, von der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die Bedrohungen enthalten, die in der Einstellung `ExcludeThreats.item_#` angegeben sind, nicht von der Untersuchung 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 verwenden, um Informationen über Ihr Netzwerk zu erhalten. 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 Anwendung 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` – Globale Ausnahmen nicht verwenden.
`UseOASExclusions`	Aktivieren der Verwendung der Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der Untersuchung.	`Yes` (Standardwert) – Ausschlüsse aus dem Schutz vor bedrohlichen Dateien verwenden. `No` – Ausnahmen für den Schutz vor bedrohlichen Dateien nicht 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 untersuchte Objekte in Archiven 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. 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.

Einstellung	Description	Werte
`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 mit minimaler Belastung des Systems. `Medium` – Eine mittlere Stufe der heuristischen Analyse bei ausgewogener Systemauslastung. `Deep` – Die gründlichste Untersuchung bei maximaler Systemauslastung. `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 Gerätenamen. Die App untersucht die Bootsektoren dieser Geräte. Der Einstellungswert darf nicht leer sein. Um die Aufgabe auszuführen, müssen Sie mindestens eine Maske für Gerätenamen angeben.	`AllObjects` – Untersuchung der Bootsektoren aller Geräte. `<device name mask>` – Bootsektoren der Geräte untersuchen, deren Namen der angegebenen Maske entsprechen. Standardwert: `/**` (beliebiger Zeichensatz im Gerätenamen, einschließlich des Zeichens `/`)
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.	Der Standardwert ist: `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 Anwendung 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_0000=*doc`
`Path`	Pfad zum Verzeichnis mit untersuchten Objekten.	`<path to local directory>` – Objekte in dem 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. `<file system type>` – Alle Ressourcen des angegebenen Dateisystemgeräts untersuchen.
Der Abschnitt **[ExcludedFromScanScope.item_#]** enthält die folgenden Parameter:		

Einstellung	Description	Werte
`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 Anwendung 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 ausschließen)
`Path`	Pfad zum Verzeichnis mit ausgeschlossenen Objekten.	`<path to local directory>` – Objekte im angegebenen Verzeichnis (einschließlich Unterverzeichnissen) von Untersuchungen ausschließen. Bei der Angabe des Pfades können Masken verwendet werden. 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/`. Der Pfad `/` ist standardmäßig angegeben. Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus. `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. `<file system type>` – Alle Ressourcen des angegebenen Dateisystemgeräts von der Untersuchung ausschließen. Remote-Verzeichnisse werden nur dann von der Untersuchung durch die Anwendung ausgeschlossen, wenn sie bereits vor dem Aufgabenstart eingebunden wurden. Remote-Verzeichnisse, die erst nach dem Aufgabenstart eingebunden wurden, werden von der Untersuchung nicht ausgeschlossen.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Aufgabe „Untersuchung von Wechseldatenträgern“

Über die Befehlszeile können Sie die Untersuchung von Wechseldatenträgern mithilfe der vordefinierten Aufgabe „Untersuchung von Wechseldatenträgern“ (`Removable_Drives_Scan`) verwalten.

Die Aufgabe *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 ausgeführt wird, überwacht die Anwendung den Anschluss von Wechseldatenträgern an das Gerät. Wenn ein Wechseldatenträger angeschlossen wird, erstellt und startet die Anwendung eine temporäre Aufgabe zur Untersuchung von Bootsektoren (Aufgabe vom `ODS`-Typ). diese Aufgabe kann nicht beendet werden Nach Abschluss der Aufgabe löscht wird sie von der Anwendung automatisch gelöscht.

Wenn Sie in den Einstellungen der Aufgabe *Untersuchung von Wechseldatenträgern* die Dateiuntersuchung aktiviert haben, startet die Anwendung auch eine oder mehrere temporäre Aufgaben zur benutzerdefinierten Untersuchung von Dateien (Aufgaben vom `ODS`-Typ). Bei Bedarf kann ein Benutzer mit Administratorrechten die Ausführung dieser Aufgaben beenden.

Wenn Sie die Einstellungen der Aufgabe *Untersuchung von Wechseldatenträgern* ändern, werden die neuen Werte nicht in bereits laufende temporäre Aufgaben übernommen. Wenn Sie die Aufgabe *Untersuchung von Wechseldatenträgern* beenden, werden bereits laufende temporäre Aufgaben nicht beendet.

Einstellungen der Aufgabe zur Untersuchung von Wechseldatenträgern

Parameter	Description	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 CDs/DVDs und Blu-ray-Discs) untersuchen. Die genaue Untersuchung wird mit den Standardeinstellungen für die Aufgabe `Scan_File` (ID: 3) durchgeführt. `QuickScan`. Nur Dateien **bestimmter Typen** auf Wechseldatenträgern (außer CDs/DVDs und Blu-ray-Discs) untersuchen. 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, 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) – Wechseldatenträger nicht untersuchen, wenn sie mit dem Gerät verbunden werden.

Parameter	Description	Werte
`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 genaue Untersuchung wird mit den Standardeinstellungen für die Aufgabe `Scan_File` (ID: 3) durchgeführt. `QuickScan`. Nur Dateien **bestimmter Typen** auf CD-/DVD-Laufwerken und Blu-ray-Discs untersuchen. 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, 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). CD-/DVD-Laufwerke und Blu-ray-Discs nicht untersuchen, wenn sie angeschlossen werden.
`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.

Container untersuchen

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 oder beenden und den Zeitplan der Aufgabe konfigurieren. Sie können die Einstellungen für die Untersuchung konfigurieren, indem Sie die Einstellungen für diese Aufgabe ändern.
- Mithilfe von Benutzeraufgaben zur Untersuchung von Containern (Aufgaben vom Typ `ContainerScan`). Sie können Benutzeraufgaben manuell starten und beenden und den Zeitplan der Aufgabe konfigurieren.
- Mit dem folgenden Befehl können Sie eine *benutzerdefinierte Untersuchung* der angegebenen Container und Images durchführen:

```
kesl-control --scan-container
```

Einstellungen der Untersuchung von Containern

Die folgende Tabelle beschreibt die Einstellungen für die Untersuchung von Containern, die bei der Untersuchung von Namespaces und Containern in Echtzeit verwendet werden.

Parameter	Description	Werte
`OnAccessContainerScanAction`	Aktion, die für einen Container ausgeführt werden soll, wenn ein infiziertes Objekt erkannt wird. Dieser Parameter ist verfügbar, wenn die Anwendung im Rahmen einer Lizenz verwendet wird, von der diese Funktion abgedeckt wird. Bei der Untersuchung von Objekten in Containern werden die Einstellungen der Aufgabe Schutz vor bedrohlichen Dateien verwendet.	`StopContainerIfFailed` (Standardwert) – der Container wird angehalten, wenn die Desinfektion oder das Löschen eines infizierten Objekts fehlgeschlagen ist. Wenn dieser Wert ausgewählt ist, hängt die für den Container ausgeführte Aktion auch vom angegebenen Wert des Parameters `ActionOnThreat` der Aufgabe Schutz vor bedrohlichen Dateien ab. Wenn der Parameter `ActionOnThreat` auf `DisinfectDeleteIfNotPossible` gesetzt ist und die Anwendung das infizierte Objekt beim Ausführen der Aktion nicht desinfizieren oder löschen kann, wird der Container gestoppt. `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 des Systems zur Verwaltung von Docker-Containern.	`Yes` (Standardwert) – System zur Verwaltung von Docker-Containern verwenden. `No` – System zur Verwaltung von Docker-Containern nicht verwenden.
`DockerSocket`	Pfad oder URI (Uniform Resource Identifier) des Docker-Sockets.	Der Standardwert ist /var/run/docker.sock.
`UseCrio`	CRI-O-Umgebung verwenden.	`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`	Podman-Tool verwenden.	`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`	runc-Tool verwenden.	`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.

Aufgabe zur Untersuchung von Containern

Die Tabelle beschreibt alle verfügbaren Werte und Standardwerte aller Einstellungen, die Sie für die Aufgabe zur Untersuchung von Containern (`Container_Scan`) angeben können.

Einstellungen der Aufgabe zur Untersuchung von Containern

Einstellung	Description	Werte
`ScanContainers`	Untersuchung von per Maske angegebenen Containern. Sie können Masken mithilfe der Einstellung `ContainerNameMask` angeben.	`Yes` (Standardwert) – Die mittels Maske angegebenen Container untersuchen. `No` – Die mittels Maske angegebenen Container nicht untersuchen.

`ContainerNameMask`	Gibt einen Namen oder eine Namensmaske an, der bzw. die einen 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).
		Beispiel für die Untersuchung eines Containers namens my_container
		`ContainerNameMask=my_container`
		Beispiel für die Untersuchung aller Container, deren Namen mit my_container beginnen
		`ContainerNameMask=my_container*`
		Beispiel für die Untersuchung aller Container, deren Namen mit my_ beginnen, dann fünf beliebige Zeichen enthalten, anschließend _container enthalten und mit einer beliebigen Zeichenfolge enden
		`ContainerNameMask=my_?????_container*`

`ScanImages`	Untersuchung von per Maske angegebenen Images. Sie können Masken mithilfe der Einstellung `ImageNameMask` angeben.	`Yes` (Standardwert) – Die anhand der Maske festgelegten Images untersuchen. `No` – Die anhand der Maske festgelegten Images nicht untersuchen.

`ImageNameMask`	Gibt einen Namen oder eine Namensmaske an, der bzw. die 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).
		Beispiel für die Untersuchung von Images mit dem Namen "my_image" und dem Tag "latest"
		`ImageNameMask=my_image:latest`
		Beispiel für die Untersuchung aller Images, deren Namen mit my_image_ beginnen und die einen beliebigen Tag 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 Anwendung hält den Container an, falls die Desinfektion oder das Löschen eines infizierten Objekts fehlschlägt. Wenn dieser Wert ausgewählt ist, hängt die für den Container ausgeführte Aktion auch vom angegebenen Wert des Parameters `ActionOnThreat` ab, der für Objekte in Containern und Images gilt (siehe untere Tabelle). Wenn der Parameter `ActionOnThreat` auf `DisinfectDeleteIfNotPossible` gesetzt ist und die Anwendung das infizierte Objekt beim Ausführen der Aktion nicht desinfizieren oder löschen kann, wird der Container gestoppt. 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 empfohlen, den Vorgang `StopContainer` auszuwählen. `StopContainer` – Die Anwendung hält den Container an, wenn ein infiziertes Objekt erkannt wird. `Skip` – Die Anwendung führt keine Aktion für Container aus, wenn ein infiziertes Objekt erkannt wird.

Einstellung	Description	Werte
`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 Anwendung führt keine Aktion für das Image aus, wenn ein infiziertes Objekt erkannt wird. `Delete` – Die Anwendung 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	Description	Werte
`ScanArchived`	Aktiviert die Untersuchung von Archiven (einschließlich selbstentpackender sfx-Archive). Die Anwendung 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 untersuchen. Wenn für den Parameter `ActionOnThreat` der Wert `DisinfectDeleteIfNotPossible` angegeben und eine Desinfizierung nicht möglich ist, löscht die Anwendung 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 Nur-Text-Format untersuchen. `No` (Standardwert) – E-Mail-Nachrichten im 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.

Einstellung	Description	Werte
`ActionOnThreat`	Auswahl der Aktion, welche die Anwendung für infizierte Objekte ausführen soll.	`DisinfectDeleteIfNotPossible` (Desinfizieren. Entfernen, wenn Desinfektion fehlschlägt) – Die Anwendung versucht, das infizierte Objekt zu desinfizieren und speichert eine Kopie des Objekts im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), löscht die Anwendung das Objekt. `DisinfectInformIfNotPossible` (Desinfizieren. Informieren, wenn Desinfektion fehlschlägt) – Die Anwendung versucht, das infizierte Objekt zu desinfizieren und speichert eine Kopie des Objekts im Backup-Speicher. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), speichert die Anwendung Informationen darüber im Protokoll. `Inform` (Informieren) – Die Anwendung unternimmt keinen Versuch, das infizierte Objekt zu desinfizieren oder zu löschen. Informationen über das infizierte Objekt werden im Protokoll gespeichert. Der Standardwert ist: `DisinfectDeleteIfNotPossible`.
`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, von Untersuchungen ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht von der Untersuchung ausschließen.

`ExcludeMasks.item_#`	Ausnahme 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, welche die in der Einstellung `ExcludeThreats.item_#` angegebenen Bedrohungen enthalten, von der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die Bedrohungen enthalten, die in der Einstellung `ExcludeThreats.item_#` angegeben sind, nicht von der Untersuchung 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 verwenden, um Informationen über Ihr Netzwerk zu erhalten. 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 Anwendung 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` – Globale Ausnahmen nicht verwenden.

Einstellung	Description	Werte
`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 untersuchte Objekte in Archiven 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. 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. 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 mit minimaler Belastung des Systems. `Medium` – Eine mittlere Stufe der heuristischen Analyse bei ausgewogener Systemauslastung. `Deep` – Die gründlichste Untersuchung bei maximaler Systemauslastung. `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.
`QueueScanTasks`	Geplante Untersuchungsaufgaben verzögern, wenn eine zuvor gestartete geplante Untersuchung noch ausgeführt wird. Kaspersky Endpoint Security reiht geplante Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Eine Untersuchungsaufgabe soll beispielsweise um 18:00 Uhr und um 20:00 Uhr ausgeführt werden. Die für 20:00 Uhr geplante Untersuchungsaufgabe wird verzögert, wenn die Untersuchung um 18:00 Uhr noch ausgeführt wird. Die verzögerte Aufgabe wird ausgeführt, nachdem die Aufgabe um 18:00 Uhr beendet wurde.	`Yes`, um geplante Untersuchungsaufgaben in die Warteschlange einzureihen, wenn die aktuelle Untersuchung noch ausgeführt wird. `No` (Standardwert), um geplante Untersuchungsaufgaben auch dann auszuführen, wenn die aktuelle Untersuchung noch ausgeführt wird.

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:

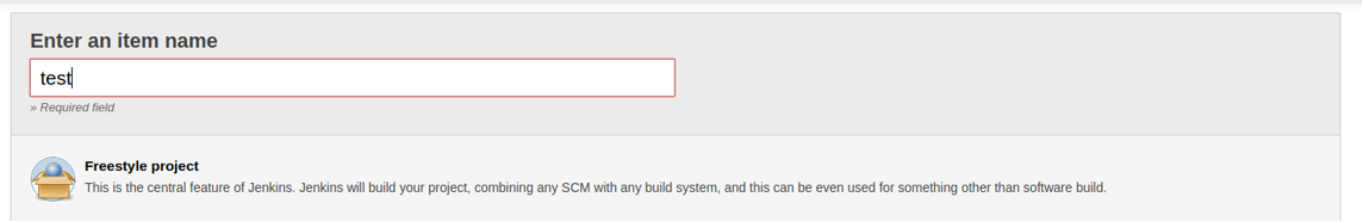
1. Installieren Sie Kaspersky Endpoint Security auf einem Jenkins-Node.
2. Installieren Sie Docker Engine auf einem Jenkins-Node.

   Weitere Informationen finden Sie in der Dokumentation zu Docker Engine.
3. Gewähren Sie dem Jenkins-Benutzer Administratorrechte für Kaspersky Endpoint Security:

   ```
   kesl-control --grant-role admin <Jenkins user name>
   ```
4. Fügen Sie einen Jenkins-Benutzer zur Gruppe „docker“ hinzu:

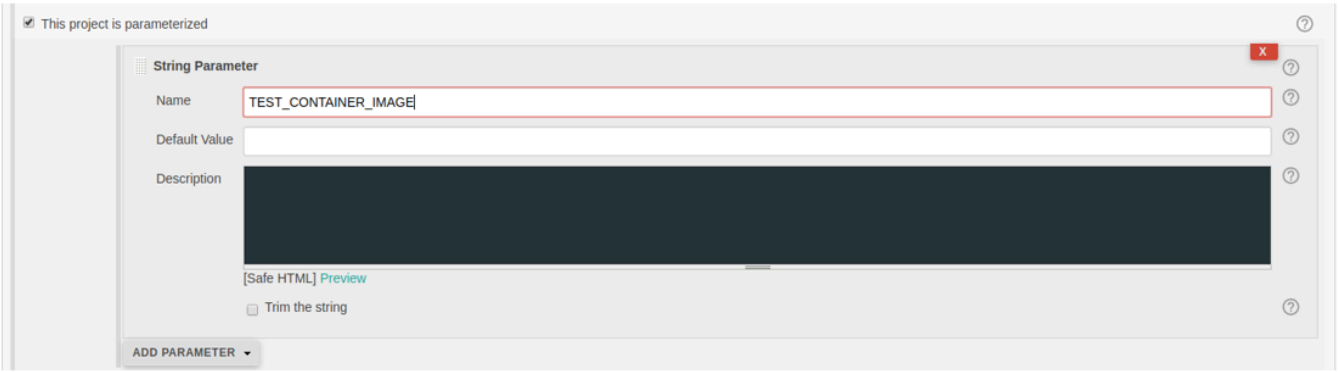
   ```
   sudo usermod -aG docker <Jenkins user name>
   ```

   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 verwenden oder Docker-Container auf andere Weise starten, speichern Sie die ID des laufenden 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. Um ein Docker-Image aus einem Repository zu untersuchen, verwenden Sie das folgende Skript:

```
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 den Build-Job.

Aufgabe zum Schutz vor Verschlüsselung

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.

Parameter	Description	Werte
`ActionOnDetect`	Aktiviert die Blockierung nicht vertrauenswürdiger Geräte	`Block` (Standardwert) – Blockierung nicht vertrauenswürdiger Geräte aktivieren. `Notify` – 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, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, aus dem Schutzbereich. 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 die Werte 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 Anwendung 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.	Der Standardwert ist: `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 Anwendung 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 schützen).
`Path`	Pfad zum Verzeichnis mit den geschützten Objekten.	`< Pfad zum lokalen Verzeichnis >` – Ein lokales Verzeichnis schützen, das über SMB/NFS erreichbar ist. Bei der Angabe des Pfades können Masken verwendet werden. `AllShared` (Standardwert) – Alle über SMB/NFS freigegebenen Ressourcen schützen. `Shared:SMB` – Ressourcen schützen, die über SMB erreichbar sind. `Shared:NFS` – Ressourcen schützen, die über NFS erreichbar sind.
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.	Der Standardwert ist: `All objects`.

Parameter	Description	Werte
`UseScanArea`	Schließt den angegebenen Bereich von dem Schutz aus.	`Yes` (Standardwert) – Den 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 Anwendung 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 Masken verwendet werden. `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.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Aufgabe zur Verhaltensanalyse

Über die Befehlszeile können Sie die Verhaltensanalyse von Anwendungen im Betriebssystem mithilfe der vordefinierten Aufgabe „Verhaltensanalyse“ (`Behavior_Detection`) verwalten.

Die Aufgabe "Verhaltensanalyse" wird standardmäßig ausgeführt. Sie können die Aufgabe manuell starten und beenden.

Sie können die Einstellungen für die Verhaltensanalyse konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zur Verhaltensanalyse ändern.

Parameter	Description	Werte
`UseTrustedPrograms`	Prozesse von der Untersuchung ausschließen.	`Yes` – Aktivität der angegebenen Prozesse von der Untersuchung ausschließen. `No` (Standardwert) – Alle Prozesse untersuchen.
`TaskMode`	Aktion, die von der App ausgeführt werden, wenn böswillige Aktivitäten im Betriebssystem erkannt werden.	`Block` (Standardwert) – Beendet den Prozess der Anwendung, die böswillige Aktivitäten ausführt. `Notify` – Beendet den Prozess, der böswillige Aktivitäten ausführt, nicht, sondern protokolliert nur die Erkennung bösartiger Aktivitäten im Ereignisprotokoll.
TelemetrySource	Zusätzliche Parameter für die Erfassung von Telemetriedaten, die an integrierten Detection and Response-Lösungen gesendet werden. Der Parameter `UseTelemetryMonopolyMode` wird nur angewendet, wenn für den Parameter `TelemetrySource` der Wert `Default` angegeben wurde.	`Default` (Standardwert) – Zur Erfassung von Telemetriedaten wird die eBPF-Technologie und der auditd-Dienst verwendet. `OnlyEBPF` – Zur Erfassung von Telemetriedaten wird nur die eBPF-Technologie verwendet.
UseTelemetryMonopolyMode	Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`True` (Standardwert) – Die Anwendung "Kaspersky Endpoint Security" verwendet den Dienst "auditd" im exklusiven Modus. `False` bedeutet, dass der Dienst auditd im nicht-exklusiven Modus verwendet wird.
Der Abschnitt **[TrustedPrograms.item_#]** enthält Prozesse, die von der Untersuchung durch die Verhaltensanalyse ausgeschlossen sind. Kaspersky Endpoint Security überwacht die Aktivität dieser Prozesse nicht.		
`ProgramPath`	Pfad des auszuschließenden Prozesses.	`< vollständiger Pfad zum Prozess >` – Prozess im angegebenen lokalen Verzeichnis nicht untersuchen. Bei der Angabe des Pfades können Masken verwendet werden.
`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`	Wird verwendet, um die Aktivität des angegebenen Prozesses von der Untersuchung auszuschließen.	`Yes` (Standardwert) – Schließt die Aktivität des angegebenen Prozesses von der Untersuchung aus. `No` – Schließt die Aktivität des angegebenen Prozesses nicht von der Untersuchung aus.

Parameter	Description	Werte
`UseTrustedProgramForDetects`	Wird verwendet, um die Aktivität des angegebenen Prozesses während der Ausführung der Komponente "Verhaltensanalyse" von der Untersuchung auszuschließen.	`Yes` – Schließt die Aktivität des angegebenen Prozesses während der Ausführung der Komponente "Verhaltensanalyse" von der Untersuchung aus. `No` (Standardwert) – Schließt die Aktivität des angegebenen Prozesses während der Ausführung der Komponente "Verhaltensanalyse" nicht von der Untersuchung aus.
`UseTrustedProgramForMDRAndEDR`	Ausnahme des Prozesses von den Telemetriedaten, die von den Komponenten MDR und EDR Expert (on-premise) erfasst werden. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`Yes` – Aktivität dieses Prozesses von den Telemetriedaten ausschließen, die von den Komponenten MDR und EDR Expert (on-premise) erfasst werden. `No` (Standardwert) – Schließt keine Prozessaktivitäten aus den Telemetriedaten, die durch MDR und EDR Expert(on-premise) gesammelt werden, aus.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Exploit-Prävention

In der Befehlszeile können Sie die Exploit-Prävention mithilfe der Einstellungen der vordefinierten Aufgabe Verhaltensanalyse (`Behavior_Detection`) verwalten.

Sie können die Einstellungen für die Exploit-Prävention konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zur Verhaltensanalyse (siehe folgende Tabelle) ändern.

Parameter	Description	Werte
`UseAEP`	Aktivieren der Komponente Exploit-Prävention.	`Yes` aktiviert die Exploit-Prävention. `No` (Standardwert) – Die Exploit-Prävention ist deaktiviert.
`AEPMode`	Aktion, welche die Anwendung beim Erkennen eines Exploits ausführen soll.	`Block` (Standardwert) – Bösartige Aktionen von Exploits werden blockiert und Informationen darüber im Ereignisprotokoll aufgezeichnet. `Notify` – Es werden keine Aktionen von Exploits blockiert, sondern nur Informationen über die Erkennung eines Exploits im Ereignisprotokoll aufgezeichnet.
Der Abschnitt **[AEPExclusions.item_#]** enthält die Untersuchungsausschlüsse der Exploit-Prävention.		
`Enabled`	Aktiviert die Verwendung von Ausnahmen aus der Untersuchung durch die Exploit-Prävention.	`Yes` (Standardwert) – die Ausnahme für die Exploit-Prävention verwenden. `No` – Verwendet keine Ausnahmen aus der Untersuchung der Exploit-Prävention.
`DetectName`	Schließt ein Objekt nach dem Namen der in im Objekt gefundenen Bedrohungen von der Untersuchung aus. Bevor Sie die Werte dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseDetectName` 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. Den vollständigen Namen der im Objekt gefundenen Bedrohung finden Sie im Protokoll der Anwendung oder auf der Website https://threats.kaspersky.com.
`Hash`	Schließt eine Datei, in der eine Bedrohung erkannt wurde, anhand ihrer Hash-Summe von der Untersuchung aus. Bevor Sie die Werte dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseHash` aktiviert ist.	
`HashType`	Typ der Hash-Summe der Datei, anhand dessen die Datei mithilfe des Parameters `Hash` von der Untersuchung ausgeschlossen werden soll.	`Md5` – Typ der Hash-Summe ist MD5. `Sha256` – Typ der Hash-Summe ist SHA256.
`Path`	Schließt eine Datei, in der eine Bedrohung erkannt wurde, anhand ihres Pfads von der Untersuchung aus. Bevor Sie die Werte dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UsePath` aktiviert ist.	`< vollständiger Pfad zur Datei oder zum lokalen Verzeichnis >` – die Datei oder Objekte im angegebenen Verzeichnis (einschließlich Unterverzeichnissen) von der Untersuchung ausschließen. Bei der Angabe des Pfades können Sie die Zeichen `*` und `?` verwenden.
`UseDetectName`	Aktiviert den Ausschluss von Objekten mit Bedrohungen, die durch die Einstellung `DetectName` festgelegt sind, aus der Untersuchung.	`Yes` (Standardwert) – Objekte, die Bedrohungen enthalten, die in den Parametern `DetectName` angegeben sind, von der Untersuchung ausschließen. `No` – Objekte, die Bedrohungen enthalten, die in den Parametern `DetectName` angegeben sind, nicht von der Untersuchung ausschließen.
`UseHash`	Aktiviert das Ausschließen einer Datei, in der eine Bedrohung erkannt wurde, anhand ihrer Hash-Summe von der Untersuchung. Die Hash-Summe der Datei wird mittels des Parameters `Hash` angegeben.	`Yes` (Standardwert) – Schließt eine Datei, in der eine Bedrohung erkannt wurde, anhand ihrer Hash-Summe von der Untersuchung aus. `No` – Schließt eine Datei, in der eine Bedrohung erkannt wurde, nicht anhand ihrer Hash-Summe von der Untersuchung aus.
`UsePath`	Aktiviert das Ausschließen einer Datei, in der eine Bedrohung erkannt wurde, anhand ihres Pfads von der Untersuchung. Der Pfad der Datei wird mittels des Parameters `Path` angegeben.	`Yes` (Standardwert) – Schließt eine Datei, in der eine Bedrohung erkannt wurde, anhand ihres Pfads von der Untersuchung aus. `No` – Schließt eine Datei, in der eine Bedrohung erkannt wurde, nicht anhand ihres Pfads von der Untersuchung aus.

Arbeiten mit dem Kaspersky Security Network

Über die Befehlszeile können Sie die Verwendung von Kaspersky Security Network mithilfe des Parameters `UseKSN` in den allgemeinen Anwendungseinstellungen aktivieren und deaktivieren.

Sie können den Wert der Einstellung `UseKSN` mithilfe von Befehlszeilenoptionen oder einer Konfigurationsdatei ändern, die alle allgemeinen Programmeinstellungen 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:

`<Extended/Basic>`: Kaspersky Security Network-Modus.

`--accept-ksn`: Option, die 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 <path to the configuration file> [--json] [--accept-ksn]
```

wobei:

`--file <path to the configuration file>` ist der vollständige Pfad zur Konfigurationsdatei mit den allgemeinen Programmeinstellungen, in der der erforderliche `UseKSN`-Wert 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 Anwendung, den Import aus einer Datei im INI-Format auszuführen. Wenn der Import fehlschlägt, wird ein Fehler angezeigt.

`--accept-ksn`: Option, die 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 Kaspersky Endpoint Security auf einem Client-Gerät installiert ist und über Richtlinien verwaltet wird, kann der Wert der Einstellung `UseKSN` nur mithilfe von Kaspersky Security Center geändert werden. Wenn die Anwendung 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 herstellen

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, verwendet Kaspersky Endpoint Security Kaspersky Security Network. Es können Informationen aus der Wissensdatenbank abgerufen werden und anonyme Statistikdaten sowie Informationen über die Typen und Quellen der Bedrohungen werden gesendet.
- Wenn als Status *Standardmäßiger KSN-Modus* angezeigt wird, verwendet Kaspersky Endpoint Security Kaspersky Security Network und 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 als Status *KSN wird nicht verwendet* angezeigt wird, verwendet Kaspersky Endpoint Security Kaspersky Security Network nicht.

In der Zeile **Infrastrukturlösung von Kaspersky Security Network** werden Informationen zu der Infrastrukturlösung angezeigt, die für die Arbeit mit den Reputationsdatenbanken von Kaspersky verwendet wird: *KSN* oder *KPSN*.

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 Anwendung 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.

Aktivieren oder Deaktivieren des Cloud-Modus

Der *Cloud-Modus* ist ein Modus zur Ausführung von Kaspersky Endpoint Security, in dem die Anwendung 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 Anwendungseinstellungen aktivieren oder deaktivieren.

Sie können die Einstellung `CloudMode` mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen App-Einstellungen enthält, oder mithilfe von Befehlszeilenoptionen.

Der Cloud-Modus der Anwendung ist bei aktivierter Verwendung von Kaspersky Security Network verfügbar.

Aufgabe zum Schutz vor BadUSB-Angriffen

Über die Befehlszeile können Sie den Schutz vor BadUSB-Angriffen mithilfe der vordefinierten Aufgabe „Schutz vor BadUSB-Angriffen“ (`Bad_USB`) verwalten.

Die Aufgabe "Schutz vor BadUSB-Angriffen" wird standardmäßig nicht gestartet. Sie können diese Aufgabe manuell starten und beenden.

Um die Aufgabe zum Schutz vor BadUSB-Angriffen über die Befehlszeile zu starten und zu beenden, sind die Rechte der Administrator-Rolle sind erforderlich.

Sie können die Einstellungen für den Schutz vor BadUSB-Angriffen konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zum Schutz vor BadUSB-Angriffen ändern.

Die untere Tabelle beschreibt die verfügbaren Werte und Standardwerte der Einstellungen, die Sie für die Aufgabe zum Schutz vor BadUSB-Angriffen angeben können.

Parameter der Aufgabe zum Schutz vor BadUSB-Angriffen

Parameter	Description	Werte
`MaxAuthAttempts`	Die maximale Anzahl für Versuche zur Autorisierung eines USB-Geräts, nach deren Erreichen die Anwendung das USB-Gerät sperrt. Erneute Versuche, das USB-Gerät zu autorisieren, sind erst möglich, nachdem die im Parameter `TimeoutAfterAttempts` angegebene Zeit abgelaufen ist.	Mögliche Werte: 1 – 10. Standardwert: 5.
`TimeoutAfterAttempts`	Zeitspanne, für die das USB-Gerät gesperrt wird, nachdem die durch den Parameter `MaxAuthAttempts` angegebene Anzahl erfolgloser Versuche zur Eingabe des Autorisierungscodes erreicht wurde.	Mögliche Werte: 1 – 180 (Min.) Standardwert: 5 Minuten.
`ProhibitOnScreenKeyboard`	Aktiviert oder deaktiviert die Verwendung der Bildschirmtastatur, um USB-Geräte zu autorisieren.	`Yes` – Die Anwendung verbietet die Verwendung der Bildschirmtastatur zur Autorisierung von USB-Geräten, bei denen die Eingabe eines Autorisierungscodes nicht möglich ist. `No` (Standardwert) – Die Anwendung lässt die Verwendung der Bildschirmtastatur zur Autorisierung von USB-Geräten zu, bei denen die Eingabe eines Autorisierungscodes nicht möglich ist.
`ProhibitBarcodeScanner`	Aktiviert oder deaktiviert die Anzeige des Autorisierungscodes als Barcode zur Autorisierung von USB-Geräten, bei denen die Eingabe eines Autorisierungscodes nicht möglich ist.	`Yes` (Standard) verbietet die Anzeige des Autorisierungscodes als Barcode. `No` erlaubt die Anzeige des Autorisierungscodes als Barcode.

Schutz von Verbindungen und Kommunikation über das Netzwerk

Aufgabe zum Schutz vor Web-Bedrohungen

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 die Aufgabe manuell starten und beenden.

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

Parameter	Description	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`	Untersuchung von Links anhand der Datenbank für bösartige 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`	Untersuchung von Links anhand der Datenbank für 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`	Verwendung der heuristischen Analyse zur Untersuchung von Webseiten auf Phishing-Links. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`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`	Untersuchung von Links anhand der Datenbank für Werbe-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`	Untersuchung von Links anhand der Datenbank für 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`	Verwendung der Liste mit vertrauenswürdigen 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 von Webadressen können Sie Masken verwenden. IP-Adressen können nicht mit Masken beschrieben werden.

Nützliche Artikel

So geben Sie Masken an

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).

Netzwerkverkehr untersuchen

Die Befehlszeile stellt spezielle Verwaltungsbefehle zur Verfügung, um die Einstellungen zur Untersuchung des Netzwerkverkehrs zu verwalten. Mithilfe der Befehle zur Verwaltung der Einstellungen zur Untersuchung des Netzwerkverkehrs können Sie Folgendes tun:

- Konfigurieren der Parameter für die Untersuchung des Netzwerkverkehrs.
- Ausschlüsse von der Untersuchung verschlüsselter Verbindungen anzeigen.
- Die Liste der Domänen löschen, welche die Anwendung automatisch von der Untersuchung ausgeschlossen hat.
- Die Liste der vertrauenswürdigen Stammzertifikate verwalten, die von der Anwendung bei der Untersuchung verschlüsselter Verbindungen verwendet wird.
- Konfigurieren und Anzeigen der Ausnahmen vom Abfangen des Datenverkehrs.

Einstellungen zur Untersuchung des Netzwerkverkehrs anzeigen und ändern

Mithilfe spezieller Befehle zur Verwaltung der Einstellungen zur Untersuchung des Netzwerkverkehrs können Sie Folgendes tun:

- Die aktuellen Werte der Parameter zur Untersuchung des Netzwerkverkehrs in der Konsole oder in eine Konfigurationsdatei ausgeben. Mit dieser Datei können Sie Einstellungen ändern.
- Alle Parameter zur Untersuchung des Netzwerkverkehrs anhand der Konfigurationsdatei ändern. Sie können die Konfigurationsdatei mit dem Befehl zum Ausgeben der Parameter zur Untersuchung des Netzwerkverkehrs abrufen.
- Bearbeiten Sie einzelne Einstellungen mithilfe von Befehlszeilenoptionen im Format `<Einstellungsname>=<Einstellungswert>`. Mit dem Befehl zur Ausgabe der Einstellungen zur Untersuchung des Netzwerkverkehrs können Sie die aktuellen Werte der Einstellungen abrufen.

Um die aktuellen Werte der Einstellungen zur Untersuchung des Netzwerkverkehrs in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-net-settings [--json]
```

Dabei wird `--json` angegeben, um die Einstellungen im JSON-Format auszugeben. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Um die aktuellen Werte der Einstellungen zur Untersuchung des Netzwerkverkehrs in die Datei auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-net-settings --file <path to configuration file> [--json]
```

wobei:

- `--file <path to the configuration file>` ist der Pfad zu der Datei, in der die Einstellungen für die Untersuchung des Netzwerkverkehrs 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 des Netzwerkverkehrs mithilfe einer Konfigurationsdatei:

1. Geben Sie die Parameter zur Untersuchung des Netzwerkverkehrs 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 folgenden Befehl aus:

   ```
   kesl-control --set-net-settings --file <path to the configuration file> [--json]
   ```

   wobei:

   - `--file <path to the configuration file>` ist der vollständige Pfad zur Konfigurationsdatei mit den Einstellungen für die Untersuchung des Netzwerkverkehrs.
   - `--json` wird angegeben, um die Einstellungen aus der Konfigurationsdatei im JSON-Format in die App zu importieren. Wenn Sie den Schalter `--json` nicht angeben, versucht die Anwendung, 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 des Netzwerkverkehrs werden in die Anwendung importiert.

Um die Werte der Einstellungen zur Untersuchung des Netzwerkverkehrs über die Befehlszeile zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-net-settings <parameter name>=<parameter value> [<parameter name>=<parameter value>]
```

wobei `<parameter name>=<parameter value>` der Name und Wert einer Einstellung für die Untersuchung des Netzwerkverkehrs ist.

Die Werte der angegebenen Einstellungen werden geändert.

Ausschlüsse von der Untersuchung verschlüsselter Verbindungen anzeigen

Sie können die folgenden Listen mit Ausschlüssen von der Untersuchung verschlüsselter Verbindungen anzeigen:

- Liste der vom Benutzer hinzugefügten Ausschlüsse.
- Liste der von der Anwendung hinzugefügten Ausschlüsse.
- Liste der von den Anwendungsdatenbanken abgerufenen Ausschlüsse.

Führen Sie den folgenden Befehl aus, um die Liste der von der App hinzugefügten Untersuchungsausschlüsse für verschlüsselte Verbindungen anzuzeigen:

```
kesl-control -N --query user
```

Führen Sie den folgenden Befehl aus, um die Liste der von der App hinzugefügten Untersuchungsausschlüsse für verschlüsselte Verbindungen anzuzeigen:

```
kesl-control -N --query auto
```

Führen Sie den folgenden Befehl aus, um die Liste der Untersuchungsausschlüsse für verschlüsselte Verbindungen anzuzeigen, die von den App-Datenbanken abgerufen wurden:

```
kesl-control -N --query kl
```

Führen Sie den folgenden Befehl aus, um die Liste der Domänen zu löschen, welche die App automatisch von der Untersuchung ausgeschlossen hat:

```
kesl-control [-N] --clear-web-auto-excluded
```

Liste der vertrauenswürdigen Stammzertifikate verwalten

Um ein Zertifikat zur Liste der vertrauenswürdigen Stammzertifikate hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --add-certificate <path to the certificate>
```

wobei:

`<path to the certificate>` ist der Pfad zur Zertifikatsdatei, die Sie hinzufügen möchten (im PEM- oder DER-Format).

Um ein Zertifikat aus der Liste der vertrauenswürdigen Stammzertifikate zu entfernen, führen Sie den folgenden Befehl aus:

```
kesl-control --remove-certificate <subject of the certificate>
```

Um die Liste der vertrauenswürdigen Stammzertifikate anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --list-certificates
```

Für jedes Zertifikat werden folgende Daten angezeigt:

- Zertifikatinhaber
- Seriennummer
- Zertifikataussteller
- Beginn der Gültigkeitsdauer des Zertifikats
- Ende der Gültigkeitsdauer des Zertifikats
- SHA256-Fingerabdruck des Zertifikats

Ausnahmen vom Abfangen des Datenverkehrs konfigurieren und anzeigen

Um dem Abfangen des Datenverkehrs eine Ausnahme hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --add-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port <destination
port>
```

wobei:

- `<in|out>` ist die Richtung des Datenverkehrs in der ausgeschlossenen Verbindung. Sie können eine Ausnahme für eingehenden oder ausgehenden Datenverkehr einrichten.
- `<remote IP address>` ist die IPv4- oder IPv6-Adresse des Remote-Geräts. Je nach Richtung des Datenverkehrs wird der Datenverkehr entweder von der angegebenen IP-Adresse (Ausschließen des eingehenden Datenverkehrs) oder zu der angegebenen IP-Adresse (Ausschließen des ausgehenden Datenverkehrs) ausgeschlossen.
- `<destination port>` ist je nach Richtung des Datenverkehrs:
  - Port auf dem geschützten Gerät (Ausschließen des eingehenden Datenverkehrs). Der Datenverkehr vom Remote-Gerät zu diesem Port wird vom Abfangen ausgeschlossen.
  - Port auf dem Remote-Gerät (Ausschließen des ausgehenden Datenverkehrs). Der Datenverkehr vom geschützten Gerät zu diesem Port wird vom Abfangen ausgeschlossen.

Sie können in der Ausnahme entweder nur die IP-Adresse eines Remote-Geräts oder den Zielport angeben.

> Wenn Sie für eine eingehende Ausnahme nur die IP-Adresse eines Remote-Geräts angeben (ohne Port des geschützten Geräts), wird der gesamte Datenverkehr vom Remote-Gerät vom Abfangen ausgeschlossen. Es wird empfohlen, eine solche Ausnahme nur für Datenverkehr von Geräten einzurichten, denen Sie vertrauen.

Um die Liste der konfigurierten Ausnahmen vom Abfangen des Datenverkehrs anzuzeigen, führen Sie folgenden Befehl aus:

```
kesl-control --list-bypass-endpoints
```

Für jede Ausnahme werden die folgenden Informationen angezeigt:

- Laufende Nummer der Ausnahme
- Richtung des Datenverkehrs der Verbindung
- IP-Adresse des Remote-Geräts
- Portnummer

Um eine Ausnahme vom Abfangen des Datenverkehrs zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control --remove-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

wobei:

- `<in|out>` ist die Richtung des Datenverkehrs in der ausgeschlossenen Verbindung.
- `<remote IP address>` ist die IPv4- oder IPv6-Adresse des Remote-Geräts, dessen Datenverkehr von der Überprüfung ausgenommen ist (abhängig von der Richtung des Datenverkehrs).
- `<destination port>` ist ein Port auf dem geschützten Gerät (Ausnahme für eingehenden Datenverkehr) oder ein Port auf dem Remote-Gerät (Ausnahme für ausgehenden Datenverkehr).

Aufgabe zum Schutz vor Netzwerkbedrohungen

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 die Aufgabe manuell starten und beenden.

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

Parameter	Description	Werte
`ActionOnDetect`	Auszuführende Aktion, wenn eine Netzwerkaktivität erkannt wird, die auf Netzwerkangriffe hinweist. Wenn Sie diese Einstellung von `Block` auf `Notify` ändern, wird die Liste der blockierten Geräte gelöscht.	`Notify` – Netzwerkaktivität zulassen und Informationen über erkannte 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 Anwendung 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 Anwendung 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 Anwendung blockiert wird. Standardmäßig ist die Liste leer.	`d.d.d.d` – Adresse der IPv4-Version, 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` – Adresse der IPv6-Version, 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.

Firewall-Verwaltung

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 der Firewall-Verwaltung konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe "Firewall-Verwaltung" 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 im Programm erstellten Firewall-Regeln mit dem folgenden Befehl an:

```
kesl-control -F --query
```

Parameter	Description	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

Parameter	Description	Werte
`Direction`	Richtung der überwachten Netzwerkaktivität.	`IncomingOutgoing` oder `InOut` (Standardwert) – sowohl eingehende als auch ausgehende Verbindungen überwachen. `Incoming` oder `In` – Nur eingehende Verbindungen überwachen. `Outgoing` oder `Out` – Nur ausgehende Verbindungen überwachen. `IncomingPacket` oder `InPacket` – Nur eingehende Pakete überwachen. `OutgoingPacket` oder `OutPacket` – Nur 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` – Adresse der IPv4-Version, wobei d eine Dezimalzahl von 0 bis 255 ist. `d.d.d.d – d.d.d.d` – Adressbereich der IPv4-Version. `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` – Adresse der IPv6-Version, wobei x eine hexadezimale Zahl von 0 bis ffff ist. `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` – Adressbereich der IPv6-Version. x:x:x:x:x:x:x:x/p – Subnetz von Adressen der IPv6-Version, wobei p eine Zahl von 0 bis 128 ist. **::** ist als Abkürzung zulässig.
`LocalAddress`	Netzwerkadressen der Geräte, auf denen die Anwendung 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` – Adresse der IPv4-Version, wobei d eine Dezimalzahl von 0 bis 255 ist. `d.d.d.d – d.d.d.d` – Adressbereich der IPv4-Version. `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` – Adresse der IPv6-Version, wobei x eine hexadezimale Zahl von 0 bis ffff ist. `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` – Adressbereich der IPv6-Version. x:x:x:x:x:x:x:x/p – Subnetz von Adressen der IPv6-Version, wobei p eine Zahl von 0 bis 128 ist. **::** ist als Abkürzung zulässig.
`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.		

Parameter	Description	Werte
`Address.item_#`	Gibt die IP-Adresse oder das IP-Subnetz an.	`d.d.d.d` – Adresse der IPv4-Version, 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` – Adresse der IPv6-Version, 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` – Adresse der IPv4-Version, 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` – Adresse der IPv6-Version, 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` – Adresse der IPv4-Version, 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` – Adresse der IPv6-Version, 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).

Konfigurieren der Liste der Regeln für Netzwerkpakete

Um eine Netzwerkpaketregel hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

wobei:

- `--name <rule name>` ist der Name der Netzwerkpaketregel.
- `--action <Allow|Block>` ist die Aktion, die für die in dieser Netzwerkpaketregel angegebenen Verbindungen ausgeführt werden soll.
- `--protocol <protocol>` ist das Protokoll, für das die Netzwerkaktivität überwacht werden soll.
- `--direction <direction>` ist die Richtung der überwachten Netzwerkaktivität.
- `--remote <remote address>:<port>` ist die Netzwerkadresse des Remote-Geräts. Als Remote-Adresse können Sie den Namen einer vordefinierten Netzwerkzone angeben.

- `--local <local address>:<port>` ist die Netzwerkadresse des Geräts, auf dem Kaspersky Endpoint Security installiert ist.

- `--at <index>` ist der 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.

Beispiel für das Erstellen einer Regel, die alle eingehenden und bestehenden Verbindungen zum TCP-Port 23 blockiert

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote
any
```

Beispiel für das Erstellen einer Regel, die eingehende und bestehende Verbindungen über 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 <rule name>
```

oder

```
kesl-control --del-rule --index <current index>
```

wobei:

- `--name <rule name>` ist der Name der Netzwerkpaketregel.

- `--index <current index>` ist der aktuelle 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 <rule name> --at < new index>
```

oder

```
kesl-control --move-rule --index <current index> --at <new index>
```

wobei:

- `--name <rule name>` ist der Name der Netzwerkpaketregel.

- `--index <current index>` ist der aktuelle Index der Regel in der Liste der Netzwerkpaketregeln.

- `--at <new index>` ist der neue Index der Regel in der Liste der Netzwerkpaketregeln.

Konfigurieren von Netzwerkzonen

Um eine Netzwerkadresse zur Zone hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --add-zone <zone> --address <address>
```

wobei:

- `<zone>` ist der vordefinierte Name der Netzwerkzone. Mögliche Werte: `Public`, `Local`, `Trusted`.
- `<address>` ist die Netzwerkadresse oder das Subnetz.

Um eine Netzwerkadresse aus der Zone zu löschen, führen Sie einen der folgenden Befehle aus:

```
kesl-control --del-zone <zone> --address <address>
```

oder

```
kesl-control --del-zone <zone> --index <address index in the 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.

Sicherheitskontrolle

Aufgabe zur Gerätekontrolle

Die Tabelle beschreibt alle möglichen Werte sowie die Standardwerte aller Einstellungen, die Sie für die Aufgabe Gerätekontrolle (`Device_Control`) angeben können.

Einstellung	Description	Werte
`OperationMode`	Ausführungsmodus der App beim Zugriffsversuch auf ein Gerät, auf das der Zugriff gemäß den Einstellungen der Gerätekontrolle verboten ist.	`Block` (Standard) – Die Anwendung wendet den für das Gerät oder den Bus angegebenen Zugriffsmodus an. `Notify` – Die Anwendung testet den ausgewählten Zugriffsmodus und generiert ein Ereignis über den Fund eines Zugriffsversuchs auf das Gerät.
`AllowToRequestTemporaryAccess`	Erlaubnis für das Anfragen von temporärem Zugriff auf ein blockiertes Gerät. Das Gewähren von Zugriff auf ein blockiertes Gerät ist nur dann verfügbar, wenn in der Organisation die Lösung "Kaspersky Security Center 16.1" bereitgestellt ist und das Client-Gerät eine Verbindung mit dem Administrationsserver herstellen kann.	`Yes` – dem Benutzer erlauben, in der grafischen Benutzeroberfläche des Programms oder in der Befehlszeile temporären Zugriff auf das blockierte Gerät anzufordern. `No` (Standardwert) – Verbietet dem Benutzer, temporären Zugriff auf ein blockiertes Gerät anzufordern.
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 Zugriff auf alle Festplatten. `DependsOnBus` (Standardwert) – Der Zugriff auf die Festplatte hängt vom Zugriffsmodus für die Bus-Verbindung ab, an die das Laufwerk angeschlossen ist. `Block` – Der Zugriff auf alle Festplatten ist für Benutzer blockiert (mit Ausnahme der Systemfestplatten, die von der Gerätekontrolle nicht blockiert werden). `ByRule` – Der Zugriff auf Festplatten ist abhängig von den Zugriffsregeln. `ReadOnly` – Benutzern ist nur der Lesezugriff auf Festplatten erlaubt. Schreibzugriff ist verboten.
`RemovableDrive`	Legt den Zugriffsmodus für an das Client-Gerät angeschlossene Wechseldatenträger fest.	`Allow` – Benutzer haben Zugriff auf alle Wechseldatenträger. `DependsOnBus` (Standardwert) – Der Zugriff auf den Wechseldatenträger hängt vom Zugriffsmodus für die Bus-Verbindung ab, an die das Laufwerk angeschlossen ist. `Block` – Benutzer haben keinen Zugriff auf Wechseldatenträger. `ByRule` – Der Zugriff auf Wechseldatenträger ist abhängig von den Zugriffsregeln. `ReadOnly` – Benutzern ist nur der Lesezugriff auf Wechseldatenträger erlaubt. Schreibzugriff ist verboten.
`FloppyDrive`	Zugriffsmodus für die mit einem Client-Gerät verbundenen Diskettenlaufwerke. Die Anwendung blockiert keine Diskettenlaufwerke, die über den ISA-Bus mit dem Client-Gerät verbunden sind.	`Allow` — Benutzer dürfen auf Diskettenlaufwerke zugreifen. `DependsOnBus` (Standardwert): Der Zugriff auf das Diskettenlaufwerk hängt von dem Zugriffsmodus ab, der für den Bus festgelegt ist, über den es verbunden ist. `Block` — Der Zugriff auf Diskettenlaufwerke ist für Benutzer gesperrt. `ByRule` — Der Zugriff auf Diskettenlaufwerke hängt von den Zugriffsregeln ab. `ReadOnly` — Benutzer haben nur Lesezugriff auf Diskettenlaufwerke; der Schreibzugriff ist gesperrt.

Einstellung	Description	Werte
`OpticalDrive`	Legt den Zugriffsmodus für CD-/DVD-Laufwerke fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Zugriff auf alle CD-/DVD-Laufwerke. `DependsOnBus` (Standardwert) – Der Zugriff auf den Wechseldatenträger hängt vom Zugriffsmodus für die Bus-Verbindung ab, an die das CD-/DVD-Laufwerk angeschlossen ist. `Block` – Benutzer haben keinen Zugriff auf CD-/DVD-Laufwerke. `ByRule` – Der Zugriff auf CD-/DVD-Laufwerke ist abhängig von den Zugriffsregeln. `ReadOnly` – Benutzern ist nur der Lesezugriff auf CD/DVD-Laufwerke erlaubt. Schreibzugriff ist verboten.
`SerialPortDevice`	Legt Zugriffsmodi für Geräte fest, die über eine serielle Schnittstelle an das Client-Gerät angeschlossen sind. Die Anwendung blockiert keine Geräte, die über eine serielle Schnittstelle via ISA-Bus an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Zugriff auf alle Geräte, die über eine serielle Schnittstelle angeschlossen sind. `DependsOnBus` (Standardwert) – Der Zugriff auf ein über eine serielle Schnittstelle angeschlossenes Gerät ist abhängig vom Zugriffsmodus für die Bus-Verbindung. `Block` – Benutzer haben keinen Zugriff auf Geräte, die über eine serielle Schnittstelle angeschlossen sind.
`ParallelPortDevice`	Legt Zugriffsmodi für Geräte fest, die über eine parallele Schnittstelle an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Zugriff auf alle Geräte, die über eine parallele Schnittstelle angeschlossen sind. `DependsOnBus` (Standardwert) – Der Zugriff auf ein über eine parallele Schnittstelle angeschlossenes Gerät ist abhängig vom Zugriffsmodus für die Bus-Verbindung. `Block` – Benutzer haben keinen Zugriff auf Geräte, die über eine parallele serielle Schnittstelle angeschlossen sind.
`Printer`	Legt den Zugriffsmodus für Drucker fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Zugriff auf alle Drucker. `DependsOnBus` (Standardwert) – Der Zugriff auf den Drucker hängt vom Zugriffsmodus für die Bus-Verbindung ab, an die der Drucker angeschlossen ist. `Block` – Benutzer haben keinen Zugriff auf Drucker.
`Modem`	Legt den Zugriffsmodus für Modems fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Zugriff auf alle Modems. `DependsOnBus` (Standardwert) – Der Zugriff auf das Modem hängt vom Zugriffsmodus für die Bus-Verbindung ab, an die das Modem angeschlossen ist. `Block` – Benutzer haben keinen Zugriff auf Modems.
`TapeDrive`	Legt den Zugriffsmodus für Bandgeräte fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Zugriff auf alle Bandgeräte. `DependsOnBus` (Standardwert) – Der Zugriff auf das Bandgerät hängt vom Zugriffsmodus für die Bus-Verbindung ab, an die das Bandgerät angeschlossen ist. `Block` – Benutzer haben keinen Zugriff auf Bandgeräte.
`MultifuncDevice`	Legt den Zugriffsmodus für Multifunktionsgeräte fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Zugriff auf alle Multifunktionsgeräte. `DependsOnBus` (Standardwert) – Der Zugriff auf das Multifunktionsgerät hängt vom Zugriffsmodus für die Bus-Verbindung ab, an die das Gerät angeschlossen ist. `Block` – Benutzer haben keinen Zugriff auf Multifunktionsgeräte.
`SmartCardReader`	Legt den Zugriffsmodus für Smartcard-Leser fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Zugriff auf alle Smartcard-Leser. `DependsOnBus` (Standardwert) – Der Zugriff auf den Smartcard-Leser hängt vom Zugriffsmodus für die Bus-Verbindung ab, an die das Gerät angeschlossen ist. `Block` – Benutzer haben keinen Zugriff auf Smartcard-Leser.

Einstellung	Description	Werte
`WiFiAdapter`	Legt den Zugriffsmodus für WLAN-Adapter fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Zugriff auf alle WLAN-Adapter. `DependsOnBus` (Standardwert) – Der Zugriff auf den WLAN-Adapter ist abhängig vom Zugriffsmodus für die Bus-Verbindung. `Block` – Benutzer haben keinen Zugriff auf WLAN-Adapter.
`NetworkAdapter`	Legt den Zugriffsmodus für externe Netzwerkadapter fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Zugriff auf alle externen Netzwerkadapter. `DependsOnBus` (Standardwert) – Der Zugriff auf den externen Netzwerkadapter hängt vom Zugriffsmodus für die Bus-Verbindung ab, an die der Adapter angeschlossen ist. Die Gerätekontrolle blockiert keinen Zugriff auf externe Netzwerkadapter, mit dem die Trennung des Client-Geräts vom Netzwerk vermieden werden kann.
`PortableDevice`	Legt den Zugriffsmodus für tragbare Geräte fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Zugriff auf alle tragbaren Geräte. `DependsOnBus` (Standardwert) – Der Zugriff auf das tragbare Gerät hängt vom Zugriffsmodus für die Bus-Verbindung ab, an die das Gerät angeschlossen ist. `Block` – Benutzer haben keinen Zugriff auf tragbare Geräte.
`BluetoothDevice`	Legt den Zugriffsmodus für Bluetooth-Geräte fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Zugriff auf alle Bluetooth-Geräte. `DependsOnBus` (Standardwert) – Der Zugriff auf das Bluetooth-Gerät hängt vom Zugriffsmodus für die Bus-Verbindung ab, an die das Gerät angeschlossen ist. `Block` – Benutzer haben keinen Zugriff auf Bluetooth-Geräte.
`ImagingDevice`	Legt den Zugriffsmodus für Bildverarbeitungsgeräte fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Zugriff auf alle Bildverarbeitungsgeräte. `DependsOnBus` (Standardwert) – Der Zugriff auf das Bildverarbeitungsgerät hängt vom Zugriffsmodus für die Bus-Verbindung ab, an die das Gerät angeschlossen ist. `Block` – Benutzer haben keinen Zugriff auf Bildverarbeitungsgeräte.
`SoundAdapter`	Legt den Zugriffsmodus für Soundadapter fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Zugriff auf alle Soundadapter. `DependsOnBus` (Standardwert) – Der Zugriff auf den Soundadapter hängt vom Zugriffsmodus für die Bus-Verbindung ab, an die das Gerät angeschlossen ist. `Block` – Benutzer haben keinen Zugriff auf Soundadapter.
`InputDevice`	Legt den Zugriffsmodus für Eingabegeräte (Tastatur, Maus, Touchpad usw.) fest, die an das Client-Gerät angeschlossen sind.	`Allow` – Benutzer haben Zugriff auf alle Eingabegeräte. `DependsOnBus` (Standardwert) – Der Zugriff auf das Eingabegerät hängt vom Zugriffsmodus für die Bus-Verbindung ab, an die das Gerät angeschlossen ist. `Block` – Benutzer haben keinen Zugriff auf 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) – Benutzer haben Zugriff auf alle USB-Geräte. `Block` – Benutzer haben keinen Zugriff auf USB-Geräte.

Einstellung	Description	Werte
`FireWire`	Zugriffsmodus für Geräte, die über eine FireWire-Schnittstelle an das Client-Gerät angeschlossen sind.	`Allow` (Standardwert) – Benutzer haben Zugriff auf alle Geräte, die über eine FireWire-Schnittstelle angeschlossen sind. `Block` – Benutzer haben keinen Zugriff auf Geräte, die über eine FireWire-Schnittstelle angeschlossen sind.
Der Abschnitt **[TrustedDevices.item_#]** enthält vertrauenswürdige Geräte.		
`DeviceId`	Gibt die ID oder ID-Maske eines vertrauenswürdigen Geräts an.	Sie können die Masken * (beliebige Zeichenfolge) oder ? (ein beliebiges Zeichen) verwenden, um die Geräte-ID anzugeben. Beispiele: *Um den Zugriff auf alle USB-Geräte außer dem angegebenen zu verweigern, geben Sie die folgenden Parameter an:* Im Abschnitt `[DeviceBus]` den Parameter `USB=Block` Im Abschnitt `[TrustedDevices.item_#]` den Parameter `DeviceId=<device ID>` *Um den Zugriff auf sämtliche USB-Geräte zu verweigern, und nur auf USB-Laufwerke zuzulassen, geben Sie die folgenden Parameter an:* Im Abschnitt `[DeviceBus]` den Parameter `USB=Block` Im Abschnitt `[TrustedDevices.item_#]` den Parameter `DeviceId=USBSTOR*`
`Comment`	Kommentar zum angegebenen vertrauenswürdigen Gerät.	—
Der Abschnitt **[TrustedDevices.item_#.Principals.item_#]** enthält die Regeln für den Zugriff auf ein vertrauenswürdiges Gerät.		
`Principal`	Der Benutzer oder die Benutzergruppe, für die das Gerät als vertrauenswürdig gilt. Wenn für den Zugriffstyp auf das Gerät "Nur Lesen" angegeben ist und Sie einem bestimmten Benutzer ein vertrauenswürdiges Gerät zuweisen, wird der zugewiesene Benutzer ignoriert und das Gerät steht mit dem Zugriff "Schreiben" allen Benutzern zur Verfügung.	`\Everyone` (Standardwert) – Das Gerät gilt für alle Benutzer als vertrauenswürdig. `<user name>` ist der Name eines lokalen Benutzers oder Domänenbenutzers, für den das Gerät vertrauenswürdig ist (ohne den vollständigen Namen mit Domäne anzugeben, wenn das System die Eingabe von Benutzernamen in diesem Format zulässt, oder im Format <Domänenname>\`<user name>` oder `<user name>` @<Domänenname>). `@<group name>` ist der Name der (lokalen oder Domänen-)Benutzergruppe, für die das Gerät vertrauenswürdig ist.
Der Abschnitt **[Schedules.item_#]** enthält die Zugriffszeitpläne für Geräte. Sie können einen Zeitplan nur für Festplatten, Wechseldatenträger, Diskettenlaufwerke und CD/DVD-Laufwerke konfigurieren.		
`ScheduleName`	Gibt den Namen eines Zeitplans an. Der Zeitplanname muss eindeutig sein.	Der Standardwert ist: `Default`. Der Zeitplan `Default` ermöglicht allen Benutzern jederzeit den vollständigen Zugriff auf Geräte, sofern der Zugriff über den Verbindungsbus für den jeweiligen Gerätetyp zulässig ist. Der `Default` Zeitplan kann nicht gelöscht werden.

Einstellung	Description	Werte

`DaysHours`	Gibt die Zeitintervalle für einen Zeitplan an.	`All` (Standardwert) – Der Zeitplan gilt für 24/7 (keine zeitliche Begrenzung).
		`<weekday>` – Wochentage. Sie können sowohl die vollständigen Namen der Wochentage als auch deren Abkürzungen verwenden (bspw. können Sie für Montag die Werte `Mo`, `Mon` oder `Monday` angeben). Als Wochentage können Sie Intervalle oder bestimmte Tage angeben. Die Woche beginnt am Sonntag.
		`<hour>` – Stunden [0:24]. Als Stunden können Sie nur Intervalle angeben.
		Beispiel für den Zeitplan schedule_1, der von Sonntag bis Samstag von 0 bis 11 Uhr, von 12 bis 15 Uhr und von 16 bis 24 Uhr gültig ist.
		`[Schedules.item_0001]`
		`ScheduleName=schedule_1`
		`DaysHours=Su-Sa:0..11,12..15,16..24`
		Beispiel für den Zeitplan schedule_2, der für die folgenden Intervalle gültig ist: donnerstags von 12 bis 14 Uhr und freitags von 2 bis 15 Uhr sowie von 16 bis 24 Uhr.
		`[Schedules.item_0002]`
		`ScheduleName=schedule_2`
		`DaysHours=Th:12..14;Fr:2..15,16..24`
		Beispiel für den Zeitplan schedule_3, der 24 Stunden am Tag, 7 Tage die Woche gültig ist
		`[Schedules.item_0003]`
		`ScheduleName=schedule_3`
		`DaysHours=All`

Der Abschnitt **[HardDrivePrincipals.item_#]** enthält die Zugriffsregeln für Festplatten. Für Festplatten muss immer mindestens ein Zeitplan aktiviert sein. Einer Festplatte können mehrere Zugriffsregeln zugewiesen werden. Es können auch mehrere Zeitpläne für einen Benutzer oder eine Benutzergruppe angegeben werden. Bei Konflikten in 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` (Standardwert) – Die Zugriffsregel gilt für alle Benutzer. `<user name>` ist der Name des lokalen Benutzers, für den die Zugriffsregel gilt. `@<group name>` ist der Name der Benutzergruppe, für die die Zugriffsregel gilt.
`[HardDrivePrincipals.item_#.AccessRules.item_#]` enthält die Parameter für die Zugriffsregel.		
`UseRule`	Gibt an, ob die Regel aktiviert oder deaktiviert ist.	`Yes` (Standardwert) – Die Zugriffsregel ist aktiviert. `No` – Die Zugriffsregel ist deaktiviert.
`ScheduleName`	Gibt den im Abschnitt `[Schedules.item_#]` festgelegten Zeitplan an.	Der Standardwert ist: `Default`.
`Access`	Gibt den Zugriffstyp an.	`Allow` (Standardwert) – Der Zugriff auf Festplatten ist erlaubt. `Block` – der Zugriff auf Festplatten wird blockiert.
Der Abschnitt **[RemovableDrivePrincipals.item_#]** enthält die Zugriffsregeln für Wechseldatenträger. Für Wechseldatenträger muss immer mindestens ein Zeitplan aktiviert sein. Einem Wechseldatenträger können mehrere Zugriffsregeln zugewiesen werden. Es können auch mehrere Zeitpläne für einen Benutzer oder eine Benutzergruppe angegeben werden. Bei Konflikten in 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` (Standardwert) – Die Zugriffsregel gilt für alle Benutzer. `<user name>` ist der Name des lokalen Benutzers, für den die Zugriffsregel gilt. `@<group name>` ist der Name der Benutzergruppe, für die die Zugriffsregel gilt.
`[RemovableDrivePrincipals.item_#.AccessRules.item_#]` enthält die Parameter für die Zugriffsregel.		
`UseRule`	Gibt an, ob die Regel aktiviert oder deaktiviert ist.	`Yes` (Standardwert) – Die Zugriffsregel ist aktiviert. `No` – Die Zugriffsregel ist deaktiviert.
`ScheduleName`	Gibt den im Abschnitt `[Schedules.item_#]` festgelegten Zeitplan an.	Der Standardwert ist: `Default`.

Einstellung	Description	Werte
`Access`	Gibt den Zugriffstyp an.	`Allow` (Standardwert) – Der Zugriff auf Festplatten ist erlaubt. `Block` – Der Zugriff auf Wechseldatenträger wird blockiert.
Der Abschnitt **[FloppyDrivePrincipals.item_#]** enthält die Zugriffsregeln für Diskettenlaufwerke. Für Diskettenlaufwerke muss immer mindestens ein Zeitplan aktiviert sein. Einem Diskettenlaufwerk können mehrere Zugriffsregeln zugewiesen werden. Es können auch mehrere Zeitpläne für einen Benutzer oder eine Benutzergruppe angegeben werden. Bei Konflikten in 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` (Standardwert) – Die Zugriffsregel gilt für alle Benutzer. `<user name>` ist der Name des lokalen Benutzers, für den die Zugriffsregel gilt. `@<group name>` ist der Name der Benutzergruppe, für die die Zugriffsregel gilt.
`[FloppyDrivePrincipals.item_#.AccessRules.item_#]` enthält die Parameter für die Zugriffsregel.		
`UseRule`	Gibt an, ob die Regel aktiviert oder deaktiviert ist.	`Yes` (Standardwert) – Die Zugriffsregel ist aktiviert. `No` – Die Zugriffsregel ist deaktiviert.
`ScheduleName`	Gibt den im Abschnitt `[Schedules.item_#]` festgelegten Zeitplan an.	Der Standardwert ist: `Default`.
`Access`	Gibt den Zugriffstyp an.	`Allow` (Standardwert) – Der Zugriff auf Diskettenlaufwerke ist erlaubt. `Block` – Der Zugriff auf Diskettenlaufwerke wird 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 mehrere Zugriffsregeln zugewiesen werden. Es können auch mehrere Zeitpläne für einen Benutzer oder eine Benutzergruppe angegeben werden. Bei Konflikten in 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` (Standardwert) – Die Zugriffsregel gilt für alle Benutzer. `<user name>` ist der Name des lokalen Benutzers, für den die Zugriffsregel gilt. `@<group name>` ist der Name der Benutzergruppe, für die die Zugriffsregel gilt.
`[OpticalDrivePrincipals.item_#.AccessRules.item_#]` enthält die Parameter für die Zugriffsregel.		
`UseRule`	Gibt an, ob die Regel aktiviert oder deaktiviert ist.	`Yes` (Standardwert) – Die Zugriffsregel ist aktiviert. `No` – Die Zugriffsregel ist deaktiviert.
`ScheduleName`	Gibt den im Abschnitt `[Schedules.item_#]` festgelegten Zeitplan an.	Der Standardwert ist: `Default`.
`Access`	Gibt den Zugriffstyp an.	`Allow` (Standardwert) – Der Zugriff auf CD-/DVD-Laufwerke ist erlaubt. `Block` – Der Zugriff auf CD-/DVD-Laufwerke wird blockiert.

Web-Kontrolle

Sie können die Web-Kontrolle über die Befehlszeile mithilfe der vordefinierten Aufgabe zur Web-Kontrolle (`Web_Control`) verwalten.

Die Aufgabe zur Web-Kontrolle ist standardmäßig gestoppt. Sie können die Aufgabe manuell starten und beenden.

Sie können Einstellungen der Web-Kontrolle konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zur Web-Kontrolle ändern.

Sie können Einstellungen der Web-Kontrolle auch mithilfe der Verwaltungsbefehle der Web-Kontrolle anzeigen und konfigurieren.

Aufgabe „Web-Kontrolle“

Die folgende Tabelle beschreibt alle verfügbaren Werte und Standardwerte aller Einstellungen, die Sie für die Aufgabe zur Web-Kontrolle (`Web_Control`) angeben können.

Einstellungen der Aufgabe "Web-Kontrolle"

Parameter	Description	Werte
`WebControlDefaultAction`	Die Aktion der Standardregel, welche die Webkontrolle ausführt, wenn sie einen Versuch erkennt, auf Webressourcen zuzugreifen, die nicht durch andere Regeln abgedeckt sind.	`Allow` (Standardwert) – Gewährt Zugriff auf die Webressourcen. `Block` – Verbietet den Zugriff auf 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. Der Relgename muss eindeutig sein.	
`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) – Gewährt Zugriff auf die Webressource. `Block` – Verbietet den Zugriff auf die Webressource. `Notify` – 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.
`Enabled`	Ausführungsstatus der Zugriffsregel für die Webressourcen:	`Yes` – Die Regel ist aktiviert und wird während der Ausführung der Web-Kontrolle angewendet. `No` (Standardwert) – Die Regel ist deaktiviert und wird während der 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) – Adressfilter für Webressourcen in der Regel nicht anwenden. Stattdessen wird 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 Masken verwenden.
`UseCategories`	Anwenden von Filtern nach Inhaltskategorien und nach Datentypkategorien in der Regel.	`None` (Standardwert) – Keine Inhaltsfilter für die Webressourcen anwenden. `ContentOnly` – Filter nach Inhaltskategorien in der Regel anwenden. `FormatOnly` – Filter nach Datentypkategorien in der Regel anwenden. `ContentAndFormat` – Filter nach Inhaltskategorien und nach Datentypkategorien in der Regel anwenden.
`[Rules.item_#.ContentCategories.item_#]`	Abschnitt zur Angabe der Inhaltskategorie.	–

Parameter	Description	Werte
`ContentCategory`	Inhaltskategorie.	`AdultContent, AlcoholTobaccoNarcotics, Violence, Profanity, Weapons, ChatForum, WebMail, OnlineShops, SocialNets, Recruitment, HttpQueryRedirection, CreditCards, PoliceDecision, SoftwareAudioVideo, TechnologyElectronics, GamblingLotteriesSweepstakes, InternetCommunicationMedia, CryptocurAndMining, LegislationBE, ECommerce, ComputerGames, Religions, News, Torrents, FileSharing, AudioAndVideo, BankSites, Blogs, DatingSites, LegislationRF, LegislationGlobal, SexuallyExplicit, Sexuality, AITools`
`[Rules.item_#.FormatCategories.item_#]`	Abschnitt zur Angabe der Datentypkategorien.	–
`FormatCategory`	Datentypkategorie	`Video` – Video `Audio` – Audiodaten `OfficeDocument` – Dateien von 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 der Regel anwenden. `No` (Standardwert) – Filter nach Benutzern nicht anwenden. Stattdessen wird die Regel auf alle Benutzer angewendet.
`[Rules.item_#.Principals.item_#]`	Abschnitt zum Angeben der Benutzer, für welche die Zugriffsregel für die Webressourcen gelten soll.	
`Name`	Ein Benutzer oder eine Gruppe von Benutzern, für welche die Zugriffsregel für Webressourcen gilt.	`<username>` ist der Name des Benutzers, für den die Regel gilt. `@<groupname>` ist der Name der Benutzergruppe, für die die Regel gilt. Standardwert: die Zugriffsregel für die Webressourcen wird auf alle Benutzer angewendet.
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 Masken verwenden.
Der Abschnitt **[Schedules.item_#]** enthält den Anwendungszeitplan der Regel.		
`Id`	ID des Zeitplans, die im Abschnitt `[Rules.item_#]` verwendet wird.	`1 - 999999` `Default` -ID des Zeitplans `0` (Standardwert), der sicher stellt, dass die Regel ohne zeitliche Einschränkungen ausgeführt wird, d. h. sie ist immer aktiv.

Parameter	Description	Werte
`Name`	Gibt den Namen eines Zeitplans an.	
`DaysHours`	Gibt die Zeitintervalle für einen Zeitplan an.	`<weekday>` – Wochentage. Sie können sowohl die vollständigen Namen der Wochentage als auch deren Abkürzungen verwenden (bspw. können Sie für Montag die Werte `Mo`, `Mon` oder `Monday` angeben). Als Wochentage können Sie Intervalle oder bestimmte Tage angeben. Die Woche beginnt am Sonntag. `<hour>` – Stunden [0:24]. Für Stunden können Sie nur Intervalle 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 <path to the configuration file>] [--json]
```

wobei:

`--file <path to the configuration file>` ist der vollständige Pfad zur Konfigurationsdatei, in die Sie die Einstellungen ausgeben möchten.

`--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 <path to the configuration file>] [--json]
```

wobei:

`--file <path to the configuration file>` ist der vollständige Pfad zur Konfigurationsdatei, aus der Sie die Einstellungen importieren möchten.

`--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
```

Programmkontrolle

Über die Befehlszeile können Sie die Programmkontrolle mithilfe der vordefinierten Aufgabe „Programmkontrolle“ (`Application_Control`) verwalten.

Standardmäßig wird die Aufgabe "Programmkontrolle" nicht ausgeführt. Sie können die Aufgabe manuell starten und beenden.

Sie können die Einstellungen der Programmkontrolle auf dem Gerät konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zur Programmkontrolle ändern.

Wenn Sie die Liste der erlaubten Apps ändern oder den Start aller Apps oder von Apps, die den Betrieb von Kaspersky Endpoint Security beeinflussen, verbieten, führen Sie beim Ändern der Aufgabeneinstellungen mithilfe der Konfigurationsdatei oder mithilfe von Befehlszeilenoptionen folgenden Befehl aus:

```
kesl-control --set-settings --accept
```

Sie können Einstellungen der Programmkontrolle auch mit den Verwaltungsbefehlen der Programmkontrolle konfigurieren:

- Listen mit Kategorien erstellen und bearbeiten.
- Anzeigen der Listen mit den in der Anwendung erstellten Kategorien.
- Regelliste der Programmkontrolle konfigurieren.

Aufgabe zur Programmkontrolle

Die Tabelle beschreibt alle möglichen Werte und Standardwerte aller Einstellungen, die Sie für die Aufgabe zur Programmkontrolle (`Application_Control`) angeben können.

Einstellungen der Aufgabe zur App-Kontrolle

Parameter	Description	Werte
`AppControlMode`	Ausführungsmodus der Komponente "Programmkontrolle".	`AllowList` – Kaspersky Endpoint Security verbietet allen Benutzern den Start aller Anwendungen, außer der in den Regeln für die Programmkontrolle angegebenen. `DenyList` (Standardwert) – Kaspersky Endpoint Security erlaubt allen Benutzern den Start aller Anwendungen, außer der in den Regeln für die Programmkontrolle angegebenen.
`AppControlRulesAction`	Aktion, die Kaspersky Endpoint Security ausführen soll, wenn ein Versuch erkannt wird, eine Anwendung zu starten, die den festgelegten Regeln entspricht.	`ApplyRules` (Standardwert) – Kaspersky Endpoint Security wendet die Regeln für die Programmkontrolle 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 Anwendung 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 Anwendung anwenden, wenn die Anwendung mindestens eine Einschlussbedingung erfüllt. `No` (Standardwert) – Regel nicht auf die Anwendung anwenden, selbst wenn die Anwendung die Einschlussbedingung erfüllt.
`IncludeFileNames.item_#`	Der Name einer ausführbaren Datei, der die Regel auslöst	Bei der Angabe von Dateinamen können Sie Masken 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.
`IncludeHashes.item_#`	SHA256-Hash einer ausführbaren Datei, der die Regel auslöst	Es ist nur SHA256 zulässig.

Parameter	Description	Werte
`UseExcludes`	Verwendung von Ausschlussbedingungen, um die Regel auszulösen	`Yes` – Regel nicht auf eine Anwendung anwenden, wenn die Anwendung mindestens eine Ausschlussbedingung oder keine der Einschlussbedingungen erfüllt. `No` (Standardwert) – Regel auf die Anwendung anwenden, selbst wenn die Anwendung die Ausschlussbedingung erfüllt.
`ExcludeFileNames.item_#`	Der Name einer ausführbaren Datei, der die Regel auslöst	Bei der Angabe von Dateinamen können Sie Masken 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.
`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 Programmkontrolle für den Ausführungsmodus *Allow-Liste* (*AllowList*). Jeder Abschnitt [AllowListRules.item_#] enthält folgende Einstellungen:		
`Description`	Regelbeschreibung für die App-Kontrolle	
`AppControlRuleStatus`	Statusvarianten einer Regel der Programmkontrolle:	`On` (Standardwert) – Die Regel ist aktiviert und Kaspersky Endpoint Security wendet diese Regel während der Programmkontrolle an. `Off` – Die Regel wird während der Programmkontrolle 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 Anwendungen erlaubt oder verboten ist.		
`Access`	Der Zugriffstyp, der einem Benutzer oder einer Benutzergruppe zugewiesen wird.	`Allow` (Standardwert) – Start der Anwendung zulassen. `Block` – Start der Anwendung verbieten.
`Principal`	Benutzer oder Benutzergruppe, für welche die Regel der App-Kontrolle zutrifft	`\Everyone` (Standardwert) – Die Regel gilt für alle Benutzer. `< Benutzername >` ist der Name des Benutzers, für den die Regel gilt. `@< Gruppenname >` ist der Name der Benutzergruppe, für die die Regel gilt.
Der Abschnitt **[DenyListRules.item_#]** enthält eine Liste mit Regeln für die Programmkontrolle 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 Programmkontrolle:	`On` (Standardwert) – Die Regel ist aktiviert und Kaspersky Endpoint Security wendet diese Regel während der Programmkontrolle an. `Off` – Die Regel wird während der Programmkontrolle 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 zu erstellenden App-Kategorie, für welche die Regel angewendet wird. Als Kategorie kann die Liste der "Golden Image"-Anwendungen angegeben werden.	
Der Abschnitt **[DenyListRules.item_#.ACL.item_#]** listet die Benutzer auf, denen der Start von Anwendungen erlaubt oder verboten ist.		
`Access`	Der Zugriffstyp, der einem Benutzer oder einer Benutzergruppe zugewiesen wird.	`Allow` – Start der Anwendung erlauben. `Block` (Standardwert) – Start der Anwendung verbieten.

Parameter	Description	Werte
`Principal`	Benutzer oder Benutzergruppe, für welche die Regel der App-Kontrolle zutrifft	`\Everyone` (Standardwert) – Die Regel gilt für alle Benutzer. `< Benutzername >` ist der Name des Benutzers, für den die Regel gilt. `@< Gruppenname >` ist der Name der Benutzergruppe, für die die Regel gilt.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/dir/*/file*/` oder `/dir/file*/`.

Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.

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 Programmkontrolle (`Application_Control`).
- unter Verwendung des Befehls kesl --set-categories und der Konfigurationsdatei für die Kategorieeinstellungen.

Um eine Programmkategorie zu erstellen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-categories --file <path to the configuration file>
```

wobei:

`--file <path to the configuration file>` ist der Pfad zur Konfigurationsdatei mit den Kategorieeinstellungen.

Die Datei mit den Kategorieeinstellungen sollte die folgende Struktur haben:

```
[
   {
      "Exclude" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the
executable file>)" ],
      "GUID" : "<unique category identifier>",
      "Include" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the
executable file>)" ],
      "Name" : "<category name 1>"
   },
 {
      "Exclude" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the
executable file>)" ],
      "GUID" : "<unique category identifier>",
      "Include" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the
executable file>)" ],
      "Name" : "<category name 2>"
```

```
    }
]
```

Zur Angabe des Dateinamens in den Feldern `Exclude` und `Include` können Sie Masken verwenden.

Die Einstellung `Name` ist erforderlich. Wenn Sie den Namen der Kategorie nicht angeben, wird sie nicht erstellt oder wird gelöscht. Die Einstellung `GUID` ist ebenfalls erforderlich. Wenn Sie sie nicht angeben, wird eine Fehlermeldung angezeigt und die Kategorie wird nicht erstellt. Der Parameter `GUID` muss ohne Bindestriche angegeben werden.

Um eine Liste mit den erstellten App-Kategorien zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-categories [--names <category name 1> <category name 2> ... <category name N>] --file <path to the configuration file>
```

wobei:

- `<category name 1> <category name 2> ... <category name N>` sind die Namen der Kategorien, für die Sie Informationen bearbeiten 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 <path to the configuration file>` ist der Pfad zur Konfigurationsdatei mit den Kategorieeinstellungen.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/dir/*/file*/` oder `/dir/file*/`.

Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.

Eine Liste mit Kategorien anzeigen

Über die Befehlszeile können Sie mithilfe des folgenden Befehls zur Verwaltung der Programmkontrolle eine Liste der erstellten Programmkategorien anzeigen: `kesl-control --get-categories`.

Die Liste der erstellten Kategorien enthält die folgenden Kategorien:

- Kategorien, die Kaspersky Security Center erstellte wurden.
- Kategorien, die in den Einstellungen der Aufgabe "Programmkontrolle" 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 Programmkategorien anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-categories [--file <path to the configuration file>] [--json]
```

wobei:

- `--file <path to the configuration file>` ist der vollständige Pfad zur Konfigurationsdatei, in die Sie die Einstellungen ausgeben möchten.
- `--json` – Gibt die Einstellungen im JSON-Format aus.

Kaspersky Endpoint Security zeigt folgende Informationen zu jeder Programmkategorie 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 bestimmten Programmkategorien anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-categories [--names <category name 1> <category name 2> ... <category name N>] [--file <path to the configuration file>] [--json]
```

wobei:

- `<category name 1> <category name 2> ... <category name N>` sind die Namen der Kategorien, für die Sie Informationen anzeigen möchten. Wenn Sie Informationen mehrerer Kategorien anzeigen möchten, geben Sie die Kategorienamen durch ein Leerzeichen getrennt an.
- `--file <path to the configuration file>` – vollständiger Pfad zur JSON-Konfigurationsdatei, in die die Kategorieliste exportiert wird.
- `--json` – Gibt die Einstellungen im JSON-Format aus.

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 Programmkontrolle

Um eine Liste mit den Regeln der Programmkontrolle anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 21 [--file <path to the configuration file>] [--json]
```

wobei:

- `--file <path to the configuration file>` ist der vollständige Pfad zur Konfigurationsdatei, in die Sie die Einstellungen ausgeben möchten.
- `--json` – Gibt Daten im JSON-Format aus.

Kaspersky Endpoint Security zeigt folgende Informationen zu Regeln der Programmkontrolle an:

- Ausführungsmodus der Komponente "Programmkontrolle".
- Aktion, die von der Programmkontrolle ausgeführt wird, wenn ein Versuch erkannt wird, ein Programm zu starten, das der konfigurierten Regel entspricht.
- Beschreibung der Regel der Programmkontrolle (falls vorhanden).
- Betriebsstatus der Regel der Programmkontrolle.
- Name der Programmkategorie, für die die Regel gilt.
- Der Zugriffstyp, der einem Benutzer oder einer Benutzergruppe zugewiesen wird.
- Benutzer oder Benutzergruppe, für welche die Regel der App-Kontrolle zutrifft

Um die Liste mit den Programmkategorien und den Regeln der Programmkontrolle zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 21 [--file <path to the configuration file>] [--json]
```

wobei:

- `--file <path to the configuration file>` ist der vollständige Pfad zur Konfigurationsdatei, aus der Sie die Einstellungen importieren möchten.
- `--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 konfigurieren

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 oder beenden und den Zeitplan der Aufgabe konfigurieren. Sie können die Einstellungen für die Untersuchung konfigurieren, indem Sie die Einstellungen für diese Aufgabe ändern.

- Mithilfe von Benutzeraufgaben zur Inventarisierung (Aufgaben vom Typ `InventoryScan`). Sie können Benutzeraufgaben manuell starten, beenden, anhalten oder fortsetzen und den Zeitplan für den Aufgabenstart konfigurieren.

Sie können die Liste der Anwendungen, die auf einem Gerät als Ergebnis der Ausführung der Inventarisierungsaufgabe erkannt wurden, mithilfe der Befehle zur Verwaltung der Programmkontrolle anzeigen.

Inventarisierungsaufgabe

Die Tabelle beschreibt alle möglichen Werte sowie die Standardwerte aller Einstellungen, die Sie für die Inventarisierungsaufgabe (`Inventory_Scan`) angeben können.

Einstellungen der Inventarisierungsaufgabe

Parameter	Description	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.
`GoldenImageAction`	Die Aktion, die Kaspersky Endpoint Security nach Abschluss der Inventarisierungsaufgabe mit der Programmkategorie „Goldene Kategorie“ ausführen muss: Sie können die Kategorie "Golden Image" in Regeln der Programmkontrolle verwenden.	`DoNothing` (Standard) – die Programmkategorie „Goldene Kategorie“ nach Abschluss der Inventarisierung nicht ändern. `Create` – erkannte Anwendungen zur Programmkategorie „Goldene Kategorie“ hinzufügen. Wenn die Kategorie nicht vorhanden ist, wird sie erstellt. Wenn eine Kategorie existiert, wird die Liste der darin enthaltenen Anwendungen aktualisiert. `Remove` – die Programmkategorie „Goldene Kategorie“ leeren. Die Kategorie wird sofort nach dem Start der Aufgabe geleert, ohne dass eine Inventarisierung der Dateien auf dem Gerät durchgeführt wird.
Der Abschnitt **[ScanScope.item_#]** enthält die folgenden Parameter:		
`AreaDesc`	Beschreibung des Inventarisierungsbereichs. Die maximale Länge einer Zeichenfolge, die mit dieser Einstellung angegeben werden kann, beträgt 4096 Zeichen.	Der Standardwert ist: `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.

Parameter	Description	Werte
`AreaMask.item_#`	Einschränkung des Inventarisierungsbereichs. Im Inventarisierungsbereich untersucht die Anwendung 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 die folgenden Parameter:		
`AreaDesc`	Beschreibung des von der Inventarisierung ausgeschlossenen Bereichs.	Der Standardwert ist nicht angegeben.
`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 Anwendung 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 >` schließt Objekte im angegebenen Verzeichnis von der Untersuchung aus. Bei der Angabe des Pfades können Masken verwendet werden.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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 Anwendungen 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 Anwendungen**. Anzahl der auf dem Gerät gefundenen Anwendungen.
- Liste der Apps mit folgenden Informationen:
  - **Pfad**. Pfad zur Anwendung.
  - **Hash**. Hash-Summe der Anwendung.
  - **Typ**. Typ der App. Zum Beispiel: `Script`, `Executable`.
  - **Kategorie**. Kategorien, zu denen die Anwendung gehört (falls sie zuvor erstellt wurden). Sie können die Liste der erstellten Programmkategorien mithilfe des folgenden Befehls anzeigen:

    ```
    kesl-control --get-categories
    ```

Wenn Sie eine neue Kategorie hinzufügen, werden deren Informationen in der Liste der Apps nicht automatisch aktualisiert. Um die Liste der Anwendungen zu aktualisieren, müssen Sie die Inventarisierungsaufgabe neu starten.

Aufgabe zur Überwachung der Systemintegrität

Über die Befehlszeile können Sie die Überwachung der Systemintegrität in Echtzeit mithilfe der vordefinierten Aufgabe „Überwachung der Systemintegrität“ (`System_Integrity_Monitoring`) verwalten. Der Aufgabentyp `OAFIM`.

Die Aufgabe "Überwachung der Systemintegrität" wird standardmäßig nicht gestartet. Sie können die Aufgabe manuell starten und beenden.

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 Systemintegrität beim Zugriff

Parameter	Description	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 die Werte 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.

Parameter	Description	Werte
Der Abschnitt [ScanScope.item_#] enthält die Überwachungsbereiche der Aufgabe zur Überwachung der Systemintegrität. 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 Masken verwendet werden. Standardwert: /opt/kaspersky/kesl/
`AreaMask.item_#`	Einschränkung des Überwachungsbereichs. Im Überwachungsbereich untersucht die Anwendung nur Objekte, 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 überwacht)
Der Abschnitt **[ExcludedFromScanScope.item_#]** enthält Objekte, die aus 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 Masken verwendet werden. Der Standardwert ist nicht angegeben.
`AreaMask.item_#`	Einschränkung des Ausschlussbereichs von der Überwachung. Im Ausschlussbereich von der Überwachung schließt die Anwendung 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 von der Überwachung ausschließen).

Nützliche Artikel

So geben Sie Masken an

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.

Aufgabe zur Prüfung der Systemintegrität

Sie können über die Befehlszeile eine Prüfung der Systemintegrität auf einem Gerät ausführen, indem Sie benutzerdefinierte Aufgaben zur Prüfung der Systemintegrität (`System_Integrity_Monitoring`) verwenden. Der Aufgabentyp `ODFIM`.

Sie können Benutzeraufgaben manuell starten, beenden, anhalten oder 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

Parameter	Description	Werte
`RebuildBaseline`	Aktivieren Sie die Neuerstellung der Baseline nach Abschluss der Aufgabe *Prüfung der Systemintegrität*.	`Yes` – Aktualisiert die Baseline jedes Mal nach Abschluss der Aufgabe *Prüfung der Systemintegrität*. `No` (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 die Werte 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:		

Parameter	Description	Werte
`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 Masken verwendet werden. Standardwert: /opt/kaspersky/kesl/
`AreaMask.item_#`	Einschränkung des Überwachungsbereichs. Im Überwachungsbereich untersucht die Anwendung nur Objekte, 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 überwacht)
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 Masken verwendet werden. Der Standardwert ist nicht angegeben.
`AreaMask.item_#`	Einschränkung des Ausschlussbereichs von der Überwachung. Im Ausschlussbereich von der Überwachung schließt die Anwendung 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 von der Überwachung ausschließen).

Nützliche Artikel

So geben Sie Masken an

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.

Schutz vor komplexen Bedrohungen und gezielten Angriffen

Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)

Über die Befehlszeile können Sie die Integration von Kaspersky Endpoint Security mit der Lösung Kaspersky Endpoint Detection and Response Expert (on-premises) mithilfe der vordefinierten Aufgabe *Kaspersky Endpoint Detection and Response Expert (on-premises) (KATAEDR)* verwalten.

Diese Aufgabe ermöglicht Ihnen außerdem die Konfiguration der Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA). Für die Integration in Kaspersky Endpoint Detection and Response Expert (on-premise) müssen Sie den *EDR Expert (on-premise)*-Integrationsmodus auswählen und die Integrationseinstellungen nach Bedarf verwalten.

Sie können die Einstellungen für die Integration in Kaspersky Endpoint Detection and Response Expert (on-premises) verwalten, indem Sie die Einstellungen der vordefinierten Aufgabe ändern.

Standardmäßig wird die Aufgabe *Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)* nicht gestartet. Sie können die Aufgabe manuell starten und beenden.

Sie können die Zertifikate verwalten, die für die Verbindung mit OSMP-Servern verwendet werden, mithilfe der Befehle zur Verwaltung der Komponente EDR Expert (on-premise).

Einstellungen der Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)

In der folgenden Tabelle werden die Einstellungen der vordefinierten Aufgabe „Integration in Kaspersky Endpoint Detection and Response Expert (on-premises) (`KATAEDR`)“ beschrieben, die Sie bei der Integration in Kaspersky Endpoint Detection and Response Expert (on-premises) verwalten können.

Diese Aufgabe ermöglicht Ihnen außerdem die Konfiguration der Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA). Für die Integration in Kaspersky Endpoint Detection and Response Expert (on-premise) müssen Sie in den Aufgabeneinstellungen den Integrationsmodus *EDR Expert (on-premise)* (`Mode=EDRExpertOnPrem`) auswählen.

Parameter	Description	Wert
`Mode`	Modus der Integration. Bei der Integration in Kaspersky Endpoint Detection and Response Expert (on-premise) interagiert das Programm Kaspersky Endpoint Security mit Servern auf der OSMP-Plattform. Bei einer Integration mit Kaspersky Endpoint Detection and Response (KATA) kommuniziert Kaspersky Endpoint Security mit Servern auf der Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (Standardwert) – Integration im Modus EDR (KATA). Erlaubt die Integration mit Kaspersky Endpoint Detection and Response (KATA). Dies ist eine Komponente von Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` ist der Integrationsmodus EDR Expert (on-premise). Aktiviert die Integration in Kaspersky Endpoint Detection and Response Expert (on-premise)
`UseClientPinnedCertificate`	Aktivieren und Deaktivieren der Zwei-Wege-Authentifizierung, um die Verbindung zum OSMP-Reaktionsserver zusätzlich abzusichern. Wenn die Zwei-Wege-Authentifizierung aufseiten des OSMP-Servers für Bedrohungsreaktionen aktiviert ist, müssen Sie vor dem Start der Aufgabe die Zwei-Wege-Authentifizierung in den Einstellungen der Aufgabe *Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)* aktivieren und das Client-Zertifikat hinzufügen.	`Yes` aktiviert die Zwei-Wege-Authentifizierung, um die Verbindung zum OSMP-Server für Aktionen zur Reaktion auf Bedrohungen zusätzlich abzusichern. `No` (Standardwert) – Zwei-Wege-Authentifizierung nicht verwenden.
`SynchronizationPeriod`	Häufigkeit der Synchronisierungsanfragen an den OSMP-Reaktionsserver in Minuten.	Der Standardwert ist: `5`.
`ConnectionTimeout`	Maximale Wartezeit für eine Verbindung mit dem OSMP-Reaktionsserver in Sekunden.	Der Standardwert ist: `10`.
`RequestTimeout`	Maximale Wartezeit für eine Antwort vom OSMP-Reaktionsserver in Sekunden.	Der Standardwert ist: `10`.
`EnableTelemetry`	Senden von Daten zu Ereignissen auf Geräten (Telemetriedaten) an den OSMP-Server für die Erfassung von Telemetriedaten.	`Yes` (Standardwert) – Telemetriedaten an den OSMP-Telemetrieserver senden `No` – keine Telemetriedaten senden
Der Abschnitt **[Endpoints.item_#]** enthält die Adresse und den Port des OSMP-Reaktionsservers. Sie können mehrere Server hinzufügen.		
`Address`	Adresse des OSMP-Reaktionsservers Sie können die IP-Adresse (IPv4 oder IPv6) oder den vollqualifizierten Domänennamen (FQDN) des Servers angeben. Um sicherzustellen, dass die Kommunikation mit dem Server nicht unterbrochen wird, wenn die Anwendung bei aktivierter Netzwerkisolation des Geräts ausfällt, wird es empfohlen, die IP-Adresse des Servers anzugeben.	Der Standardwert ist: `127.0.0.1`.
`Port`	Der Port für die Verbindung zum OSMP-Reaktionsserver.	Der Standardwert ist: `443`.
Der Abschnitt **[TelemetrySettings]** enthält die allgemeinen Parameter zur Verbindung mit den OSMP-Telemetrieservern.		
`UseClientPinnedCertificate`	Aktivieren und Deaktivieren der Zwei-Wege-Authentifizierung, um die Verbindung zum OSMP-Telemetrieserver zusätzlich abzusichern. Wenn die Zwei-Wege-Authentifizierung aufseiten des OSMP-Telemetrieservers aktiviert ist, müssen Sie vor dem Start der Aufgabe die Zwei-Wege-Authentifizierung in den Einstellungen der Aufgabe *Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)* aktivieren und das Client-Zertifikat hinzufügen.	`Yes` aktiviert die Zwei-Wege-Authentifizierung, um die Verbindung zum OSMP-Telemetrieserver zusätzlich abzusichern. `No` (Standardwert) – Zwei-Wege-Authentifizierung nicht verwenden.
`ConnectionTimeout`	Maximale Wartezeit für eine Verbindung mit dem OSMP-Telemetrieserver in Sekunden.	Der Standardwert ist: `10`.
`RequestTimeout`	Maximale Wartezeit für eine Antwort vom OSMP-Telemetrieserver in Sekunden.	Der Standardwert ist: `10`.

Parameter	Description	Wert
`OnlyTaggedEvents`	Senden von Telemetriedaten nur mit IOA. Ein *Angriffsindikator (IOA)* ist eine Regel, die ein verdächtiges Verhalten im System beschreibt. Solches Verhaltens kann auf einen gezielten Angriff hinweisen. Das Programm vergleicht das aktuelle Verhalten im System mit diesen Regeln und protokolliert Ereignisse, die auf einen gezielten Angriff hindeuten. Das Programm verwendet die Technologie *Streaming-Scan*, um solche Ereignisse in Echtzeit zu verfolgen.	`Yes` – Nur Telemetriedaten senden, die mit einem Angriffsindikator versehen sind (Indicator of Attack, IOA) `No` (Standardwert) – Alle Telemetriedaten senden.
Der Abschnitt **[TelemetrySettings.Endpoints.item_#]** enthält die Adresse und den Port des OSMP-Telemetrieservers. Sie können mehrere Server hinzufügen.		
`Address`	Adresse des OSMP-Telemetrieservers. Sie können die IP-Adresse (IPv4 oder IPv6) oder den vollqualifizierten Domänennamen (FQDN) des Servers angeben. Um sicherzustellen, dass die Kommunikation mit dem Server nicht unterbrochen wird, wenn die Anwendung 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 OSMP-Telemetrieserver.	Der Standardwert ist: `443`.
Der Abschnitt **[TelemetrySettings.EventTransferSettings]** enthält die Parameter für die Datenübertragung an den OSMP-Telemetrieserver.		
`MaximumDataTransferTime`	Maximale Verzögerung beim Senden von Ereignissen an den OSMP-Telemetrieserver in Sekunden.	Der Standardwert ist: `30`.
`UseRequestCountLimits`	Begrenzen Sie die Anzahl der Anfragen. Durch diese Funktion wird die Auslastung des Computers optimiert. Wenn diese Funktion aktiviert ist, beschränkt die App die übertragenen Ereignisse. Wenn die Anzahl der Ereignisse die festgelegten Grenzwerte überschreitet, beendet Kaspersky Endpoint Security das Senden von Ereignissen.	`Yes` (Standardwert) – die Anzahl der gesendeten Ereignisse wird begrenzt `No` – die Anzahl der gesendeten Ereignisse wird nicht begrenzt
`MaximumNumberOfEventsInHour`	Maximale Anzahl an Ereignissen pro Stunde	Der Standardwert ist: `3000`.
`MaximumNumberOfEventsInPackage`	Die maximale Anzahl von Ereignissen in einem Paket.	Der Standardwert ist: `1024`.
`EventLimitExceededPercentage`	Prozentuale Überschreitung der Beschränkung der Ereignisanzahl: 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`.

Verwaltung der Zertifikate für die Verbindung mit OSMP EDR Expert (on-premise)-Servern

Zur Verwaltung der Zertifikate sind Benutzerrechte mit der Rolle Administrator erforderlich.

Sie können Befehle verwenden, um die Zertifikate zu verwalten, die für die Verbindung mit OSMP-Servern verwendet werden. Mit Zertifikaten können Sie Folgendes tun:

- Hinzufügen oder ersetzen der Zertifikate der OSMP-Server: Reaktionsserver und Telemetrieserver
- Ausgaben von Informationen über die Serverzertifikate
- Löschen der Serverzertifikate
- Hinzufügen oder ersetzen der Client-Zertifikate, die zum Schutz der Verbindung mit dem OSMP-Server verwendet werden: Reaktionsserver und Telemetrieserver
- Ausgeben von Informationen über Client-Zertifikate
- Löschen von Client-Zertifikaten

Verwaltung der Zertifikate für die Verbindung mit dem OSMP-Reaktionsserver

Um das Zertifikat des Reaktionsservers hinzuzufügen oder zu ersetzen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type response
```

wobei `<file>` der Pfad zur Datei ist, die das Serverzertifikat enthält.

So fügen Sie ein Client-Zertifikat, das zum Schutz der Verbindung mit dem Reaktionsserver verwendet wird, hinzu oder ersetzen es:

1. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file> --server-type response
   ```

   wobei `<file>` der Pfad zum Crypto-Container (PFX-Archiv) ist, der das Client-Zertifikat und den privaten Schlüssel enthält.

2. Geben Sie das Kennwort für den Crypto-Container ein

Das Client-Zertifikat wird verwendet, um die Verbindung zum OSMP-Server zusätzlich abzusichern, wenn die Überprüfung des Client-Zertifikats in den Einstellungen des OSMP-Servers aktiviert ist und in den Aufgabeneinstellungen für die *Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)* die Einstellung `UseClientPinnedCertificate` im Abschnitt `[KATAEDR]` den Wert `yes` hat.

Um Informationen über das Zertifikat des Reaktionsservers auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --query-kataedr-server-certificate --server-type response
```

Um Informationen über das Client-Zertifikat auszugeben, das zum Schutz der Verbindung mit dem Reaktionsserver verwendet wird, führen Sie folgenden Befehl aus:

```
kesl-control [-R] --query-kataedr-client-certificate --server-type response
```

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 Zertifikat des Reaktionsservers zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type response
```

Um das Client-Zertifikat, das zum Schutz der Verbindung mit dem Reaktionsserver verwendet wird, zu löschen, führen Sie folgenden Befehl aus:

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type response
```

Verwaltung der Zertifikate für die Verbindung mit dem OSMP-Telemetrieserver

Um das Zertifikat des Telemetrieservers hinzuzufügen oder zu ersetzen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type telemetry
```

wobei `<file>` der Pfad zur Datei ist, die das Serverzertifikat enthält.

So fügen Sie ein Client-Zertifikat, das zum Schutz der Verbindung mit dem Telemetrieserver verwendet wird, hinzu oder ersetzen es:

1. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file> --server-type telemetry
   ```

   wobei `<file>` der Pfad zum Crypto-Container (PFX-Archiv) ist, der das Client-Zertifikat und den privaten Schlüssel enthält.

2. Wenn der Krypto-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 OSMP-Server zusätzlich abzusichern, wenn die Überprüfung des Client-Zertifikats in den Einstellungen des OSMP-Servers aktiviert ist und in den Aufgabeneinstellungen für die *Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)* die Einstellung `UseClientPinnedCertificate` im Abschnitt `[TelemetrySettings]` den Wert `yes` hat.

Um Informationen über das Zertifikat des Telemetrieservers auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --query-kataedr-server-certificate --server-type telemetry
```

Um Informationen über das Client-Zertifikat auszugeben, das zum Schutz der Verbindung mit dem Telemetrieserver verwendet wird, führen Sie folgenden Befehl aus:

```
kesl-control [-R] --query-kataedr-client-certificate --server-type telemetry
```

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 Zertifikat des Telemetrieservers zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type telemetry
```

Um das Client-Zertifikat, das zum Schutz der Verbindung mit dem Telemetrieserver verwendet wird, zu löschen, führen Sie folgenden Befehl aus:

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type telemetry
```

Integration mit Kaspersky Endpoint Detection and Response Expert (cloud)

Über die Befehlszeile können Sie die Integration zwischen Kaspersky Endpoint Security und der Lösung Kaspersky Endpoint Detection and Response Expert (cloud) mithilfe der vordefinierten Aufgabe *Integration mit Kaspersky Endpoint Detection and Response Expert (cloud)* verwalten.

Sie können die Einstellungen der Integration mit Kaspersky Endpoint Detection and Response Expert (cloud) verwalten, indem Sie die Einstellungen der vordefinierten Aufgabe ändern.

Die Aufgabe *Integration mit Kaspersky Endpoint Detection and Response Expert (cloud)* wird standardmäßig nicht ausgeführt. Sie können die Aufgabe manuell starten und beenden.

Integrationseinstellungen für Kaspersky Endpoint Detection and Response Expert (cloud)

In der folgenden Tabelle werden die Einstellungen der vordefinierten Aufgabe zur Integration von Kaspersky Endpoint Detection and Response Expert (cloud) (`EDRExpertCloud`) beschrieben.

So rufen Sie die aktuellen Werte der Aufgabeneinstellungen ab

```
kesl-control --get-settings 39
```

So konfigurieren Sie die Aufgabeneinstellungen

```
kesl-control --set-settings 39 <parameter>=<value>
```

Parameter	Description
Integrationseinstellungen für den Antwortserver	
`UseTunnel`	Verwendung eines TCP-Tunnels für die Verbindung mit dem Response-Server. Der TCP-Tunnel wird für die Verbindung mit dem Server verwendet, wenn die Sicherheitsrichtlinie in Ihrer Infrastruktur keine direkte Verbindung mit Servern zulässt. Standardmäßig ist die Verwendung eines TCP-Tunnels deaktiviert (`No`).
`TunnelAddress`	Serveradresse (IPv4 oder IPv6) für die Verbindung mit dem Tunnel.
`TunnelPort`	Serverport für die Verbindung mit dem Tunnel.
`SynchronizationPeriod`	Häufigkeit der Synchronisierungsanfragen an den OSMP-Reaktionsserver in Minuten. Der Standardwert ist: `5`.
Integrationseinstellungen für den Server zur Erfassung von Telemetriedaten Der Abschnitt `[TelemetrySettings]` enthält allgemeine Einstellungen für die Verbindung mit OSMP-Telemetrieservern.	
`EnableTelemetry`	Senden von Daten zu Ereignissen auf Geräten (Telemetriedaten) an den OSMP-Server für die Erfassung von Telemetriedaten. Das Senden von Telemetriedaten ist standardmäßig aktiviert (`Yes`).
`OnlyTaggedEvents`	Senden von Telemetriedaten nur mit IOA. Ein *Angriffsindikator (IOA)* ist eine Regel, die ein verdächtiges Verhalten im System beschreibt. Solches Verhaltens kann auf einen gezielten Angriff hinweisen. Das Programm vergleicht das aktuelle Verhalten im System mit diesen Regeln und protokolliert Ereignisse, die auf einen gezielten Angriff hindeuten. Das Programm verwendet die Technologie *Streaming-Scan*, um solche Ereignisse in Echtzeit zu verfolgen. Standardmäßig ist das Senden von Telemetriedaten nur mit IOA deaktiviert (`No`).
`UseTunnel`	Verwendung eines TCP-Tunnels für die Verbindung mit dem Telemetrie-Erfassungsserver. Der TCP-Tunnel wird für die Verbindung mit dem Server verwendet, wenn die Sicherheitsrichtlinie in Ihrer Infrastruktur keine direkte Verbindung mit Servern zulässt. Standardmäßig ist die Verwendung eines TCP-Tunnels deaktiviert (`No`).
`TunnelAddress`	Serveradresse (IPv4 oder IPv6) für die Verbindung mit dem Tunnel.
`TunnelPort`	Serverport für die Verbindung mit dem Tunnel.
Der Abschnitt `[TelemetrySettings.EventTransferSettings]` enthält allgemeine Einstellungen für die Verbindung mit OSMP-Telemetrieservern.	
`UseRequestCountLimits`	Begrenzen Sie die Anzahl der Anfragen. Durch diese Funktion wird die Auslastung des Computers optimiert. Wenn diese Funktion aktiviert ist, beschränkt die App die übertragenen Ereignisse. Wenn die Anzahl der Ereignisse die festgelegten Grenzwerte überschreitet, beendet Kaspersky Endpoint Security das Senden von Ereignissen. Diese Option ist standardmäßig deaktiviert.
`MaximumDataTransferTime`	Maximale Verzögerung beim Senden von Ereignissen. Die App synchronisiert sich mit dem Server, um Ereignisse nach Ablauf des Synchronisierungsintervalls zu senden. Der Standardwert ist 30 Sekunden.
`MaximumNumberOfEventsInHour`	Maximale Anzahl von Ereignissen pro Stunde. Die App analysiert den Telemetriedatenstrom und schränkt das Senden von Ereignissen ein, wenn der Ereignisstrom das festgelegte Limit für Ereignisse pro Stunde überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen nach einer Stunde fort. Die Standardeinstellung ist 3.000 Ereignisse pro Stunde. Wenn die App auf einem Server installiert ist, ist der Telemetrie-Datenstrom höher. Für Server wird empfohlen, den Wert auf 60.000 Ereignisse pro Stunde zu erhöhen.
`MaximumNumberOfEventsInPackage`	Maximale Anzahl an Ereignissen pro Paket. Das Programm synchronisiert sich mit dem Server, wenn sich genügend Ereignisse im Puffer befinden. Der Standardwert beträgt 1.024 Ereignisse.
`EventLimitExceededPercentage`	Maximale Anzahl an Ereignissen eines Typs in Prozent. Die App sortiert Ereignisse nach Typ (z. B. Ereignisse des Typs „Änderungen in der Registrierung“) und schränkt die Übertragung von Ereignissen ein, wenn das Verhältnis von Ereignissen desselben Typs zur Gesamtzahl von Ereignissen den in Prozent festgelegten Grenzwert überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen fort, wenn das Verhältnis der anderen Ereignisse zur Gesamtzahl der Ereignisse wieder dem Grenzwert entspricht. Die Standardeinstellung ist 15%.

Verwalten von Verbindungszertifikaten für OSMP EDR Expert-Server (cloud)

Zur Verwaltung der Zertifikate sind Benutzerrechte mit der Rolle Administrator erforderlich.

Das Programm erhält Serveradressen und Zertifikate zum Herstellen einer vertrauenswürdigen Verbindung automatisch, nachdem Sie die Bedingungen der Vereinbarung zur Datenverarbeitung von Kaspersky Endpoint Detection and Response Expert (cloud) akzeptiert haben. Daher können Sie Zertifikate nicht mithilfe von Befehlen hinzufügen oder entfernen. Sie können Informationen zu Zertifikaten nur über die Befehlszeile anzeigen.

Verwaltung der Zertifikate für die Verbindung mit dem OSMP-Reaktionsserver

```
Informationen zum Zertifikat des Servers für die Reaktion auf Bedrohungen anzeigen
```

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type response
```

```
Informationen zum Client-Zertifikat für die Verbindung mit dem Server für die Reaktion auf Bedrohungen anzeigen
```

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type response
```

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

Verwaltung der Zertifikate für die Verbindung mit dem OSMP-Telemetrieserver

```
Anzeigen von Informationen zum Zertifikat des Servers zur Erfassung von Telemetriedaten
```

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type telemetry
```

```
Informationen zum Client-Zertifikat für die Verbindung mit dem Server für Telemetriedaten anzeigen
```

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type telemetry
```

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

Integration mit Kaspersky Endpoint Detection and Response (KATA)

Über die Befehlszeile können Sie die Integration von Kaspersky Endpoint Security mit der Komponente Kaspersky Endpoint Detection and Response (KATA) mithilfe der vordefinierten Aufgabe *Integration in Kaspersky Endpoint Detection and Response Expert (on-premises) (KATAEDR)* verwalten.

Diese Aufgabe ermöglicht es Ihnen außerdem, die Integrationseinstellungen für Kaspersky Endpoint Detection and Response Expert (on-premise) zu verwalten. Für die Integration mit Kaspersky Endpoint Detection and Response (KATA) müssen Sie in den Aufgabeneinstellungen den Integrationsmodus EDR (KATA) auswählen und die Integrationseinstellungen nach Bedarf verwalten.

Sie können Einstellungen für die Integration mit Kaspersky Endpoint Detection and Response (KATA) konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe ändern.

Standardmäßig wird die Aufgabe *Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)* nicht gestartet. Sie können die Aufgabe manuell starten und beenden.

Sie können die Zertifikate verwalten, die für die Verbindung mit KATA-Servern verwendet werden, mithilfe der Befehle zur Verwaltung der Komponente EDR Expert (on-premise).

Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA)

Die folgende Tabelle beschreibt die Einstellungen der vordefinierten Aufgabe „Integration in Kaspersky Endpoint Detection and Response Expert (on-premises) (`KATAEDR`)“, die Sie bei der Integration mit Kaspersky Endpoint Detection and Response (KATA) verwalten können.

Diese Aufgabe ermöglicht es Ihnen außerdem, die Integrationseinstellungen für Kaspersky Endpoint Detection and Response Expert (on-premise) zu verwalten. Für dir Integration mit Kaspersky Endpoint Detection and Response (KATA) müssen Sie in den Aufgabeneinstellungen den *Integrationsmodus EDR (KATA)* (Parameter `Mode=EDRKATA`) auswählen.

Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA)

Parameter	Description	Wert
`Mode`	Modus der Integration. Bei der Integration in Kaspersky Endpoint Detection and Response Expert (on-premise) interagiert das Programm Kaspersky Endpoint Security mit Servern auf der OSMP-Plattform. Bei einer Integration mit Kaspersky Endpoint Detection and Response (KATA) kommuniziert Kaspersky Endpoint Security mit Servern auf der Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (Standardwert) – Integration im Modus EDR (KATA). Erlaubt die Integration mit Kaspersky Endpoint Detection and Response (KATA). Dies ist eine Komponente von Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` ist der Integrationsmodus EDR Expert (on-premise). Aktiviert die Integration in Kaspersky Endpoint Detection and Response Expert (on-premise)

Parameter	Description	Wert
`UseClientPinnedCertificate`	Aktivieren und Deaktivieren der Zwei-Wege-Authentifizierung, um die Verbindung zum KATA-Server zusätzlich abzusichern. Wenn die Zwei-Wege-Authentifizierung aufseiten des KATA-Servers aktiviert ist, müssen Sie vor dem Starten der Aufgabe die Zwei-Wege-Authentifizierung in den Einstellungen der Aufgabe *Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)* aktivieren und das Client-Zertifikat hinzufügen.	`Yes` – Zwei-Wege-Authentifizierung verwenden, um die Verbindung zum KATA-Server zusätzlich abzusichern. `No` (Standardwert) – Zwei-Wege-Authentifizierung nicht verwenden.
`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`.
`EnableTelemetry`	Senden von Ereignisdaten (Telemetriedaten) an KATA.	`Yes` (Standardwert) – Telemetriedaten an den KATA-Server senden `No` – keine Telemetriedaten senden
Der Abschnitt **[Endpoints.item_#]** enthält die Adresse und den Port des KATA-Servers. Sie können mehrere Server hinzufügen.		
`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 Server nicht unterbrochen wird, wenn die Anwendung 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`.
Der Abschnitt **[EventTransferSettings]** enthält Parameter für die Übertragung von Daten an den KATA-Server.		
`MaximumDataTransferTime`	Maximale Verzögerung beim Senden von Ereignissen an den KATA-Server in Sekunden.	Der Standardwert ist: `30`.
`UseRequestCountLimits`	Begrenzung der Anzahl der an den KATA-Server gesendeten Ereignisse aktivieren und deaktivieren.	`Yes` (Standardwert) – die Anzahl der gesendeten Ereignisse wird begrenzt `No` – die Anzahl der gesendeten Ereignisse wird nicht begrenzt
`MaximumNumberOfEventsInHour`	Maximale Anzahl an Ereignissen pro Stunde	Der Standardwert ist: `3000`.
`MaximumNumberOfEventsInPackage`	Die maximale Anzahl von Ereignissen in einem Paket.	Der Standardwert ist: `1024`.
`EventLimitExceededPercentage`	Prozentuale Überschreitung der Beschränkung der Ereignisanzahl: 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`.

Zertifikate für die Verbindung mit dem KATA-Server verwalten

Zur Verwaltung der Zertifikate sind Benutzerrechte mit der Rolle Administrator erforderlich.

Sie können Befehle verwenden, um die Zertifikate zu verwalten, die für die Verbindung mit dem KATA-Server verwendet werden. Mit Zertifikaten können Sie Folgendes tun:

- Hinzufügen oder Ersetzen des Zertifikats des KATA-Servers
- Anzeigen von Informationen zum Serverzertifikat

- Löschen des Serverzertifikats
- Hinzufügen oder Ersetzen des Client-Zertifikats, das zum Schutz der Verbindung mit dem KATA-Server verwendet wird
- 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 <file>
```

wobei `<file>` der Pfad zur Datei ist, die das Serverzertifikat enthält.

Um ein Client-Zertifikat hinzuzufügen oder zu ersetzen:

1. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file>
   ```

   wobei `<file>` der Pfad zum Crypto-Container (PFX-Archiv) ist, der das Client-Zertifikat und den privaten Schlüssel enthält.

2. Geben Sie das Kennwort für den Crypto-Container ein

Das Client-Zertifikat wird für den zusätzlichen Schutz der Verbindung zum KATA-Server verwendet, wenn die Überprüfung des Client-Zertifikats in den Einstellungen des KATA-Servers aktiviert ist und in den Aufgabeneinstellungen der *Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)* `UseClientPinnedCertificate` auf `yes` gesetzt ist.

Um Informationen zum Serverzertifikat anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --query-kataedr-server-certificate
```

Um Informationen zum Client-Zertifikat anzuzeigen, führen Sie den folgenden Befehl aus:

```
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
```

Integration mit Kaspersky Network Detection and Response (KATA)

Über die Befehlszeile können Sie die Integration von Kaspersky Network Security mit Kaspersky Endpoint Detection and Response (KATA) mithilfe der vordefinierten Aufgabe *„Integration mit Kaspersky Network Detection and Response (KATA) (`KATANDR`)“* verwalten:

Standardmäßig wird die Aufgabe *Integration mit Kaspersky Network Detection and Response (KATA)* nicht gestartet. Sie können die Aufgabe manuell starten und beenden.

Sie können Einstellungen für die Integration mit Kaspersky Network Detection and Response (KATA) konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe ändern.

Sie können die Zertifikate verwalten, die zur Verbindung mit NDR-Servern verwendet werden, indem Sie die Befehle zur Verwaltung von NDR (KATA) verwenden.

Parameter für die Integration mit Kaspersky Network Detection and Response (KATA)

Die folgende Tabelle beschreibt alle verfügbaren Einstellungen und Standardwerte für alle Einstellungen, die Sie für die Aufgabe „Integration mit Kaspersky Network Detection and Response (KATA)“ (`KATANDR`) festlegen können.

Einstellungen der Aufgabe zur Integration mit Kaspersky Network Detection and Response (KATA)

Parameter	Description	Wert
`UseClientPinnedCertificate`	Aktivieren und Deaktivieren der Zwei-Wege-Authentifizierung, um die Verbindung zum NDR-Server zusätzlich abzusichern. Wenn die Überprüfung des Client-Zertifikats auf der Seite des NDR-Servers aktiviert ist, müssen Sie die Verwendung des Client-Zertifikats aktivieren und das Client-Zertifikat hinzufügen, bevor Sie die Aufgabe *Integration mit Kaspersky Network Detection and Response (KATA)* ausführen.	`Yes` – Zwei-Wege-Authentifizierung verwenden, um die Verbindung zum NDR-Server zusätzlich abzusichern. `No` (Standardwert) – Zwei-Wege-Authentifizierung nicht verwenden.
`SynchronizationPeriod`	Häufigkeit des Sendens von Synchronisierungsanfragen an den NDR-Server in Minuten.	Der Standardwert ist: `5`.
`ConnectionTimeout`	Die maximale Wartezeit auf eine Verbindung mit dem NDR-Server in Sekunden.	Der Standardwert ist: `10`.
`RequestTimeout`	Die maximale Wartezeit auf eine Antwort vom NDR-Server in Sekunden.	Der Standardwert ist: `10`.
Der Abschnitt **[Endpoints.item_#]** enthält die Adresse und den Port des NDR-Servers.		
`Address`	Adresse des NDR-Servers. Sie können die IP-Adresse (IPv4 oder IPv6) oder den vollqualifizierten Domänennamen (FQDN) des Servers angeben.	Der Standardwert ist: `127.0.0.1`.

Parameter	Description	Wert
`Port`	Port für die Verbindung zum NDR-Server.	Der Standardwert ist: `8081`.
Der Abschnitt **[EventTransferSettings]** enthält Parameter für die Übertragung von Ereignissen an den NDR-Server.		
`MaximumDataTransferTime`	Maximale Verzögerung beim Senden von Ereignissen an den NDR-Server in Sekunden.	Der Standardwert ist: `30`.
`MaximumNumberOfEventsInPackage`	Die maximale Anzahl von Ereignissen in einem Paket.	Der Standardwert ist: `1024`.
`UseRequestCountLimits`	Begrenzung der Anzahl der an den NDR-Server gesendeten Ereignisse aktivieren und deaktivieren.	`Yes` (Standardwert) – die Anzahl der gesendeten Ereignisse wird begrenzt `No` – die Anzahl der gesendeten Ereignisse wird nicht begrenzt
`MaximumNumberOfEventsInHour`	Maximale Anzahl an Ereignissen pro 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`.
`PingPeriod`	Häufigkeit der Abfrage von NDR-Servern in Sekunden.	Der Standardwert ist: `450`.

Zertifikate für die Verbindung mit dem NDR-Server verwalten

Zur Verwaltung der Zertifikate sind Benutzerrechte mit der Rolle Administrator erforderlich.

Sie können Befehle verwenden, um die Zertifikate zu verwalten, die für die Verbindung mit dem NDR-Server verwendet werden. Mit Zertifikaten können Sie Folgendes tun:

- Hinzufügen oder Ersetzen des Zertifikats des NDR-Servers
- Anzeigen von Informationen zum Serverzertifikat
- Löschen des Serverzertifikats
- Fügen Sie das Client-Zertifikat, das zur Sicherung der Verbindung zum NDR-Server verwendet wird, hinzu oder ersetzen Sie es.
- 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-katandr-server-certificate <file>
```

wobei `<file>` der Pfad zur Datei ist, die das Serverzertifikat enthält.

Um ein Client-Zertifikat hinzuzufügen oder zu ersetzen:

1. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control [-R] --add-katandr-client-certificate <file>
   ```

   wobei `<file>` der Pfad zum Crypto-Container (PFX-Archiv) ist, der das Client-Zertifikat und den privaten Schlüssel enthält.

2. Geben Sie das Kennwort für den Crypto-Container ein

Das Client-Zertifikat wird verwendet, um die Verbindung zum NDR-Server zusätzlich abzusichern, wenn die Überprüfung des Client-Zertifikats in den Einstellungen des NDR-Servers aktiviert ist und in den Aufgabeneinstellungen der *Integration mit Kaspersky Network Detection and Response (KATA)* die Einstellung `UseClientPinnedCertificate` auf `yes` festgelegt ist.

Um Informationen zum Serverzertifikat anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --query-katandr-server-certificate
```

Um Informationen zum Client-Zertifikat anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --query-katandr-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-katandr-server-certificate
```

Um das Client-Zertifikat zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --remove-katandr-client-certificate
```

Integration mit Sandbox

Über die Befehlszeile können Sie die Integration des Programms Kaspersky Endpoint Security mit Sandbox mithilfe der vordefinierten Aufgabe *Integration mit Sandbox* verwalten.

Die Aufgabe *Integration mit Sandbox* wird nicht standardmäßig ausgeführt. Sie können diese Aufgabe manuell starten und beenden.

Führen Sie folgenden Befehl aus, um die Aufgabe Integration mit Sandbox zu starten:

```
kesl-control --start-task 29
```

> Die Aufgabe *Integration mit Sandbox* kann nicht gestartet werden, wenn das Serverzertifikat nicht hinzugefügt wurde.

Wenn die Aufgabe *Integration mit Sandbox* gestartet wurde und der ausgewählte Modus das manuelle Senden von Dateien zur Untersuchung erlaubt (`Manual` oder `AutoAndManual`), können Sie Dateien über die Befehlszeile zur Untersuchung an Sandbox senden.

So senden Sie Dateien zur Untersuchung an Sandbox

```
kesl-control [-X] --sandbox <path>
```

wobei `<path>` der Pfad zu der Datei oder dem Verzeichnis ist, die bzw. das Sie untersuchen möchten. Sie können mehrere, durch Leerzeichen getrennte Pfade angeben.

Sie können die Einstellungen für die Integration mit Sandbox konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe ändern.

Mithilfe der Befehle zur Verwaltung der Einstellungen für die Integration mit Sandbox können Sie die Zertifikate verwalten, die für die Verbindung mit den Servern, welche die Interaktion mit Sandbox gewährleisten, verwendet werden.

Einstellungen für die Integration mit Sandbox

Die folgende Tabelle beschreibt alle verfügbaren Einstellungen und Standardwerte für alle Einstellungen, die Sie für die Aufgabe „Integration mit Sandbox“ (`Standalone_Sandbox`) festlegen können.

So konfigurieren Sie die Einstellungen für die Integration mit Sandbox

```
kesl-control --set-settings 29 Servers.item_0000.Address=<server> Servers.item_0000.Port=<port> [<setting name>=
<setting value>]
```

Parameter	Description	Wert
`UseClientCertificate`	Aktivieren und Deaktivieren der Zwei-Wege-Authentifizierung, um die Verbindung zum Sandbox-Server zusätzlich abzusichern. Wenn die Überprüfung des Client-Zertifikats auf der Seite des Sandbox-Servers aktiviert ist, müssen Sie die Verwendung des Client-Zertifikats aktivieren und das Client-Zertifikat hinzufügen, bevor Sie die Aufgabe *Integration mit Sandbox* ausführen.	`Yes` – Zwei-Wege-Authentifizierung verwenden, um die Verbindung zum Sandbox-Server zusätzlich abzusichern. `No` (Standardwert) – Zwei-Wege-Authentifizierung nicht verwenden.
`ConnectionTimeout`	Die maximale Wartezeit auf eine Verbindung mit dem Server in Sekunden.	Der Standardwert ist: `10`.
`RequestTimeout`	Die maximale Wartezeit auf eine Antwort vom Server in Sekunden.	Der Standardwert ist: `10`.
`SendingMode`	Modus zum Senden der Datei zur Untersuchung an die Sandbox	`AutoOnly` (Standardwert) – Dateien werden beim Zugriff automatisch zur Untersuchung gesendet. `Manual` – Dateien werden manuell zur Untersuchung gesendet. `AutoAndManual` – Dateien werden sowohl automatisch als auch manuell zur Untersuchung gesendet.
`QuarantineFile`	Datei nach Erkennung einer Bedrohung in die Quarantäne verschieben.	`Yes` (Standardwert) – Bei Erkennung einer Bedrohung wird die ursprüngliche Datei gelöscht und eine Kopie der Datei in die Quarantäne verschoben. `No` – Bei Erkennung einer Bedrohung wird die Datei nicht in die Quarantäne verschoben.
`ScanCriticalAreas`	Führt die Untersuchung wichtiger Bereiche bei Erkennung einer Bedrohung aus.	`Yes` (Standardwert) – Bei Erkennung einer Bedrohung wird die Untersuchung wichtiger Bereiche gestartet. `No` – Bei Erkennung einer Bedrohung wird die Untersuchung wichtiger Bereiche nicht gestartet.
`CreateIocScanTask`	Erstellt bei Erkennung einer Bedrohung eine Aufgabe zur IOC-Untersuchung.	`Yes` (Standardwert) – Bei Erkennung einer Bedrohung wird eine Aufgabe zur IOC-Untersuchung erstellt. `No` – Bei Erkennung einer Bedrohung wird keine Aufgabe zur IOC-Untersuchung erstellt.
`QuarantineFileOnIocDetected`	Objekt nach Erkennung eines Kompromittierungsindikators in die Quarantäne verschieben.	`Yes` (Standardwert) – Bei Erkennung eines Kompromittierungsindikators wird das ursprüngliche Objekt gelöscht und eine Kopie des Objekts in die Quarantäne verschoben. `No` – Bei Erkennung eines Kompromittierungsindikators wird das Objekt nicht in die Quarantäne verschoben.
`ScanCriticalAreasOnIocDetected`	Führt die Untersuchung wichtiger Bereiche bei Erkennung eines Kompromittierungsindikators aus.	`Yes` (Standardwert) – Bei Erkennung eines Kompromittierungsindikators wird die Untersuchung wichtiger Bereiche gestartet. `No` – Bei Erkennung eines Kompromittierungsindikators wird die Untersuchung wichtiger Bereiche nicht gestartet.
`Drives`	Bereiche, die auf Kompromittierungsindikatoren untersucht werden.	`Critical` (Standardwert) – Untersucht Dateien in benutzerdefinierten Verzeichnissen und Systemverzeichnissen. `System` – Untersucht alle Dateien innerhalb des Stamm-Dateisystems.
`ScheduleMode`	Ausführungsmodus der Aufgabe zur IOC-Untersuchung.	`Manually` (Standardwert) – IOC-Untersuchung manuell ausführen. `AfterTreatDetected` – IOC-Untersuchung nach Erkennung einer Bedrohung ausführen.

Parameter	Description	Wert
Der Abschnitt **[Servers.item_#]** enthält die Parameter des Sandbox-Servers.		
`Address`	Adresse des Servers. Sie können die IP-Adresse (IPv4 oder IPv6) oder den vollqualifizierten Domänennamen (FQDN) des Servers angeben.	Der Standardwert ist: `127.0.0.1`.
`Port`	Port für die Verbindung zum Server.	Der Standardwert ist: `443`.
Der Abschnitt **[SandboxTransferSettings]** enthält Parameter für die Übertragung von Dateien zur Untersuchung in Sandbox.		
`SandboxQueue`	Die maximale Größe des Verzeichnisses zum Speichern der Warteschlange für Untersuchungsanfragen in Megabyte.	Der Standardwert ist: `1024`.

Verwaltung der Zertifikate für die Verbindung mit dem Sandbox-Server

Zur Verwaltung der Zertifikate sind Benutzerrechte mit der Rolle Administrator erforderlich.

Sie können die Zertifikate, die für Verbindungen mit OSMP-Servern oder Central Node-Servern verwendet werden, die für die Interaktion mit der Sandbox (im Folgenden auch Sandbox-Server genannt) verantwortlich sind, mithilfe von Befehlen verwalten. Mit Zertifikaten können Sie Folgendes tun:

- 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 [-X] --add-sandbox-server-certificate <file>
```

wobei `<file>` der Pfad zur Datei ist, die das Serverzertifikat enthält.

Um ein Client-Zertifikat hinzuzufügen oder zu ersetzen:

1. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control [-X] --add-sandbox-client-certificate <file>
   ```

   wobei `<file>` der Pfad zum Crypto-Container (PFX-Archiv) ist, der das Client-Zertifikat und den privaten Schlüssel enthält.

2. Geben Sie das Kennwort für den Crypto-Container ein

Das Client-Zertifikat wird verwendet, um die Verbindung zum Sandbox-Server zusätzlich abzusichern, wenn die Überprüfung des Client-Zertifikats in den Einstellungen des Sandbox-Servers aktiviert ist und der Parameter `yes` in den Einstellungen der Aufgabe *Integration mit Sandbox* auf `UseClientCertificate` steht.

Um Informationen zum Zertifikat anzuzeigen, führen Sie den folgenden Befehl aus:

- für das Serverzertifikat:

  ```
  kesl-control [-X] --query-sandbox-server-certificate
  ```

- für das Client-Zertifikat:

  ```
  kesl-control [-X] --query-sandbox-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 [-X] --remove-sandbox-server-certificate
```

Um das Client-Zertifikat zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control [-X] --remove-sandbox-client-certificate
```

Integration mit Kaspersky Endpoint Detection and Response Optimum aktivieren und deaktivieren

Über die Befehlszeile können Sie die Funktionen von EDR Optimum mit dem Parameter `UseEdrOptimum` in den allgemeinen Anwendungseinstellungen aktivieren oder deaktivieren.

Sie können den Wert der Einstellung mithilfe von Befehlszeilenschaltern oder einer Konfigurationsdatei ändern, die alle allgemeinen Programmeinstellungen enthält.

Um die Komponente "EDR Optimum" anhand des Parameters über die Befehlszeile zu aktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

Um die Komponente "EDR Optimum" anhand des Parameters über die Befehlszeile zu deaktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings UseEdrOptimum=No
```

Konfigurieren der Integration von Kaspersky Managed Detection and Response

Über die Befehlszeile können Sie Folgendes tun:

- Die MDR-Komponente aktivieren oder deaktivieren.
- Die MDR-BLOB-Datei hochladen und löschen, welche die Lizenzinformationen für Kaspersky Managed Detection and Response enthält.

  Wenn Sie einen Lizenzschlüssel zum Aktivieren der MDR-Komponente verwenden, müssen Sie die MDR-BLOB-Datei nicht hochladen.

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 die MDR-Komponente mithilfe des Parameters `UseMDR` in den allgemeinen Anwendungseinstellungen aktivieren oder deaktivieren. Sie können den Wert der Einstellung mithilfe von Befehlszeilenschaltern oder einer Konfigurationsdatei ändern, die alle allgemeinen Programmeinstellungen enthält.

Der Parameter `UseMDR` kann folgende Werte annehmen:

- `Yes` – MDR-Komponente aktivieren.
- `No` – MDR-Komponente deaktivieren.

Wenn Sie die MDR-Komponente aktivieren und Kaspersky Security Network deaktiviert ist oder im Standardmodus ausgeführt wird, erscheint eine Fehlermeldung und die MDR-Komponente wird nicht aktiviert. Um die MDR-Komponente zu aktivieren, muss Kaspersky Security Center im erweiterten Modus aktiviert werden.

Sie können die MDR-BLOB-Ddatei mithilfe der Befehle zur Verwaltung der Lizenzschlüssel hochladen und löschen. Die BLOB-Datei befindet sich im ZIP-Archiv der MDR-Konfigurationsdatei.

Führen Sie den folgenden Befehl aus, um die BLOB-Datei hochzuladen:

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

Führen Sie den folgenden Befehl aus, um die BLOB-Datei zu löschen:

```
kesl-control --remove-mdr-blob
```

Nach der Aktivierung der Integration wird eine Dienstaufgabe `Mdr_Autostart_Scan` erstellt, die einmal am Tag ausgeführt wird.

Verwalten der Netzwerkisolation von Geräten

Bei einer Integration mit Detection and Response-Lösungen können Sie die folgenden Aktionen über die Befehlszeile ausführen:

- Status der Netzwerkisolation eines Geräts prüfen und die Liste mit den Ausnahmen von der Netzwerkisolation anzeigen.
- Die Netzwerkisolation des Geräts deaktivieren.

Um die Netzwerkisolation eines Geräts zu deaktivieren, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --isolation-off
```

Um den Status der Netzwerkisolation zu prüfen und die Liste mit den Ausnahmen von der Netzwerkisolation anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control [-R] --isolation-stat
```

Für die Netzwerkisolation wird einer der folgenden Statuswerte angezeigt:

- *Netzwerkisolation ist aktiviert*.
- *Netzwerkisolation ist deaktiviert*.

Parameter der Quarantäne konfigurieren

Über die Befehlszeile können Sie die Quarantäne-Einstellungen mithilfe der Optionen `QuarantineSizeLimit`, `QuarantineFillingNotification` und `QuarantineBackupFolder` in den allgemeinen Anwendungseinstellungen konfigurieren.

Sie können die Werte der Einstellungen mithilfe von Befehlszeilenschaltern oder einer Konfigurationsdatei ändern, die alle allgemeinen Programmeinstellungen enthält.

Quarantäne-Einstellungen

Parameter	Description	Wert
`QuarantineFillingNotification`	Füllstand der Quarantäne in Prozent, bei dessen Erreichen eine Ereignis über mangelnden Quarantäne-Speicher generiert werden soll. Um das Generieren von Ereignissen über den Quarantäne-Füllstand zu deaktivieren, geben Sie den Wert 0 ein.	0 – 100 0 – Das Generieren von Ereignissen über den Quarantäne-Füllstand ist deaktiviert. Standardwert: 90.
`QuarantineSizeLimit`	Maximale Größe der Quarantäne (in Megabyte). Wenn die maximale Größe des Quarantäne-Speichers erreicht ist, löscht die Anwendung die ältesten Objekte. Um die Begrenzung der Quarantäne-Größe aufzuheben, geben Sie den Wert 0 an.	0 – 4000 0 – Die Größe der Quarantäne ist nicht begrenzt. Der Standardwert ist 200, wenn die App im Standard-Modus oder im EDR Agent-Modus verwendet wird, und 100, wenn die App im Light Agent-Modus verwendet wird.
`QuarantineBackupFolder`	Pfad zum Verzeichnis, in dem die Objekte des Backups und der Quarantäne gespeichert werden. Sie können ein Verzeichnis angeben, das sich vom Standardverzeichnis unterscheidet. Die zum Speichern der Objekte des Backups und der Quarantäne verwendeten Verzeichnisse können sich auf beliebigen Geräten befinden. Es wird nicht empfohlen, Verzeichnisse zu wählen, die sich auf Remote-Geräten befindet und etwa über Samba- oder NFS-Protokolle gemountet sind. Wenn das angegebene Verzeichnis nicht existiert oder nicht verfügbar ist, verwendet die Anwendung das Standardverzeichnis.	Standardwert: /var/opt/kaspersky/kesl/common/objects-backup/ Für den Zugriff auf das Standardverzeichnis sind Root-Rechte erforderlich.

Quarantäne-Dateien über die Befehlszeile verwalten

Bei einer Integration mit Detection and Response-Lösungen können Sie anhand der Befehle zur Verwaltung der Quarantäne die folgenden Aktionen über die Befehlszeile ausführen:

- Dateien in die Quarantäne verschieben (nur bei Integration mit Kaspersky Endpoint Detection and Response Optimum oder Kaspersky Managed Detection and Response).
- Informationen über Quarantäne-Dateien anzeigen.
- Alle oder nur bestimmte Dateien aus der Quarantäne löschen.
- Datei aus der Quarantäne wiederherstellen

Die Wiederherstellung infizierter Dateien kann zu einer Infektion des Geräts führen.

Die Datei in die Quarantäne verschieben.

Um eine Datei in die Quarantäne zu verschieben, führen Sie den folgenden Befehl aus:

```
kesl-control [-Q] --put <path to the file> [--md5] [--sha256] [--save-original-file]
```

wobei:

- `<path to the file>` ist der Pfad zu der Datei, die Sie in die Quarantäne verschieben möchten.
- `--md5` – MD5-Hash der Datei, die Sie in die Quarantäne verschieben möchten.
- `--sha256` – Hash der Datei, die Sie in die Quarantäne verschieben möchten
- `--save-original-file` – Originaldatei nicht löschen. Wenn Sie diesen Schlüssel nicht angeben, wird die Originaldatei gelöscht.

  Die Originaldatei wird nur gelöscht, wenn das Konto des Benutzers über die Berechtigung zum Löschen von Objekten verfügt. Bei unzureichenden Rechten wird beim Löschen der Datei eine Fehlermeldung angezeigt.

Sie können diesen Befehl nur bei Integration mit Kaspersky Endpoint Detection and Response Optimum oder Kaspersky Managed Detection and Response ausführen.

Informationen über Quarantäne-Dateien anzeigen

Um Informationen über Quarantäne-Dateien anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control -Q --query ["<filter conditions>"] [-n <number of files>] [--json]
```

wobei:

- `<filter conditions>` gibt einen oder mehrere logische Ausdrücke im Format `< Feld > < Vergleichsoperation > '< Wert >'` an, die mit dem logischen Operator `and` kombiniert werden, um die Abfrageergebnisse einzuschränken. Wenn Sie keine Filterbedingungen angeben, zeigt die App Informationen zu allen Quarantäne-Dateien an.
- `<number of files>` ist die Anzahl der zuletzt in die Quarantäne verschobenen Dateien, die Sie anzeigen möchten. Wenn Sie den Schlüssel `-n` nicht angeben, werden die letzten 30 Dateien angezeigt. Um alle Dateien anzuzeigen, geben Sie den Wert 0 ein.
- `--json` – Gibt Daten im JSON-Format aus.

In der Zeile `ObjectId` wird die numerische ID angezeigt, welche die Anwendung der Datei zugewiesen hat, als sie in die Quarantäne verschoben wurde. Diese ID wird verwendet, um Aktionen für eine Datei auszuführen, z. B. beim Wiederherstellen oder Löschen einer Datei aus der Quarantäne.

Dateien aus der Quarantäne wiederherstellen

So stellen Sie eine Datei aus der Quarantäne unter dem ursprünglichen Namen am ursprünglichen Speicherort wieder her:

```
kesl-control -Q --restore <object identifier>
```

Dabei steht `<object identifier>` für eine numerische ID, die die Anwendung der Datei zugewiesen hat, als sie in die Quarantäne verschoben wurde.

So stellen Sie eine Datei unter einem neuen Namen in einem angegebenen Verzeichnis aus der Quarantäne wieder her:

```
kesl-control -Q --restore <object identifier> --file <path to the file>
```

Dabei steht --file `<path to the file>` für den neuen Namen der Datei und den Pfad zu dem Verzeichnis, in dem Sie die Datei speichern möchten.

Sie können eine Quarantäne-Datei nur dann in einem anderen Verzeichnis wiederherstellen, wenn Ihr Konto über Root-Rechte verfügt. Bei unzureichenden Rechten kann die Datei nur an ihrem ursprünglichen Speicherort wiederhergestellt werden.

Auf Geräten mit dem Betriebssystem Astra Linux kann im Modus für geschlossene Softwareumgebungen eine Datei nur unter dem Benutzerkonto wiederhergestellt werden, unter dem sie ins Backup verschoben wurde. Beim Wiederherstellen einer Datei erstellt die Anwendung ein Verzeichnis mit MAC-Label 3 (cnnr-Flag).

Dateien aus der Quarantäne löschen

Um ausgewählte Dateien aus der Quarantäne zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control -Q --mass-remove --query "<filter conditions>"
```

wobei `<filter conditions>` einen oder mehrere logische Ausdrücke im Format <field><comparison operation>'<value>' angibt, die mit dem logischen Operator "and" kombiniert werden, um die Abfrageergebnisse einzuschränken.

```
Beispiel für das Löschen von Dateien, deren Namen oder Pfade "test" enthalten
kesl-control -Q --mass-remove --query "FileName like '%test%'"
```

Um alle Dateien aus der Quarantäne zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control -Q --mass-remove
```

IOC-Untersuchung

Nur bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie Suche nach Kompromittierungsindikatoren anhand der IOC-Untersuchungsaufgabe über die Befehlszeile ausführen. Bei der Integration in Kaspersky Endpoint Detection and Response (on-premises) oder Kaspersky Endpoint Detection and Response (KATA) wird die IOC-Untersuchung seitens der entsprechenden Detection and Response-Lösung ausgeführt.

Um die Aufgabe IoC-Untersuchung über die Befehlszeile zu erstellen, zu konfigurieren und auszuführen, verwenden Sie den folgenden Befehl:

```
kesl-control [-T] --scan-ioc --path <path to the directory or file> [--process on|off] [--hint <regular
expression>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives
all|system|critical|custom] [--excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

wobei:

- `--path <path to the directory or file>` ist der Pfad zu einer IOC-Datei oder zu einem Verzeichnis mit IOC-Dateien mit der Erweiterung .IOC oder .XML, der für die Durchführung der Untersuchung verwendet werden soll.

  Sie können mehrere, durch Leerzeichen getrennte Pfade angeben. Sie können auch beide Arten von Pfaden (Datei und Verzeichnis) angeben.

- `--process` – Analyse der auf dem Gerät laufenden Prozesse aktivieren.

  Mögliche Argumente:

  - `on` – Analyse der auf dem Gerät ausgeführten Prozesse aktivieren (Standardwert).
  - `off` – Analyse der auf dem Gerät ausgeführten Prozesse deaktivieren.

  Wenn Sie den Parameter `--process` nicht angeben, führt die Anwendung nur dann eine Prozessanalyse durch, wenn die verwendete IOC-Datei Daten dieser Prozesse (`ProcessItem`) enthält.

- `--hint <regular expression>` ist der reguläre Ausdruck, der dem vollständigen Pfad zur zu analysierenden Datei (`FileItem`) oder zur ausführbaren Datei des zu analysierenden Prozesses (`ProcessItem`) entspricht.

  Für den regulären Ausdruck können folgende Elemente verwendet werden:

  - Meta-Zeichen: `. ^ $ |`
  - Zeichenklassen: digit, alpha, lower, upper, cntrl
  - Quantifikatoren: `* + ? {n} {n,} {n, m}`
  - Negation: `[^a-c]`
  - Geschützte Zeichen: `\a \e \f`, `\n \r \t \v \b`

- `--arpentry` – Analyse von Einträgen in der ARP-Tabelle (`ArpEntryItem`) aktivieren.

  Mögliche Argumente:

  - `on` – Analyse von Einträge in der ARP-Tabelle aktivieren (Standardwert).
  - `off` – Analyse von Einträgen in der ARP-Tabelle deaktivieren.

  Wenn Sie den Parameter `--arpentry` nicht angeben, führt die Anwendung nur dann eine Analyse der ARP-Tabelle durch, wenn die verwendete IOC-Datei Daten dieser Tabelle (`ArpEntryItem`) enthält.

  `--ports` – Analyse von Ports aktivieren, die geöffnet sind und Verbindungen empfangen können.

  Mögliche Argumente:

  - `on` – Analyse von geöffneten Ports und aktiven Verbindungen mit dem Gerät aktivieren (Standardwert).
  - `off` – Analyse von geöffneten Ports und aktiven Verbindungen mit dem Gerät deaktivieren.

  Wenn Sie den Parameter `--ports` nicht angeben, führt die Anwendung nur dann eine Portanalyse durch, wenn die verwendete IOC-Datei Daten dieser Ports (`PortItem`) enthält.

- `--system` – Analyse der Systemumgebung aktivieren.

  Mögliche Argumente:

  - `on` – Analyse der Systemumgebung aktivieren (Standardwert).
  - `off` – Analyse der Systemumgebung deaktivieren.

  Wenn Sie den Parameter `--system` nicht angeben, führt die Anwendung nur dann eine Analyse der Systemumgebung durch, wenn die verwendete IOC-Datei Daten über die Systemumgebung (`SystemInfoItem`) enthält.

- `--files` – Dateianalyse aktivieren.

  Mögliche Argumente:

  - `on` – Dateianalyse aktivieren (Standardwert).
  - `off` – Dateianalyse deaktivieren.

  Wenn Sie den Parameter `--files` nicht angeben, führt die Anwendung nur dann eine Dateianalyse durch, wenn die verwendete IOC-Datei Daten dieser Dateien (`FileItem`) enthält.

- `--drives` – zu untersuchende Bereiche.

  Mögliche Argumente:

  - `all` – alle verfügbaren Dateibereiche untersuchen.
  - `system` – Untersucht alle Dateien innerhalb des Stamm-Dateisystems.
  - `critical` – Dateien in den Benutzer- und Systemverzeichnissen untersuchen (Standardwert).
  - `custom` – nur die Dateien untersuchen, die sich in den von Ihnen angegebenen Bereichen befinden.

  Wenn Sie den Parameter `--drives` nicht angeben, analysiert die Anwendung die Dateien in den Benutzer- und Systemverzeichnissen.

- `--excludes <list of exclusions>` ist die Liste der von der Untersuchung ausgeschlossenen Pfade.

  Die in diesem Parameter angegebenen Ausnahmen sind global und gelten unabhängig von der Art des Bereichs oder der Verzeichnisliste. Diese Ausnahmen haben Vorrang vor anderen Befehlszeilenoptionen, einschließlich `--hint` und `--scope`.

  > Ausschlüsse werden als Pfade angegeben, dürfen jedoch keine rekursiven Elemente oder Masken-Symbole (wie `*`) enthalten.

  Wenn Sie den Parameter `--excludes` nicht angeben, wird die Untersuchung ohne Ausschlüsse durchgeführt.

  Sie können mehrere, durch Leerzeichen getrennte Ausschlüsse angeben.

- `--scope <list of directories>` ist die Liste der zusätzlichen Verzeichnisse, die untersucht werden sollen.

  > Diese Option ist erforderlich, wenn Sie das Argument `--drives` für die Option `custom` angegeben haben.

- `--action` – Aktion, die bei Erkennung eines Kompromittierungsindikators ausgeführt werden soll.

  Mögliche Argumente:

  - `Skip` – die Anwendung führt keine Aktionen mit dem erkannten Objekt aus, aber Informationen darüber werden in den Ergebnissen der Aufgabenausführung gespeichert (Standardwert).
  - `QuarantineFile` – die Anwendung verschiebt das erkannte Objekt in die Quarantäne.
  - `IsolateHost` – die Anwendung isoliert das Gerät, auf dem das Objekt erkannt wurde, vom Netzwerk.
  - `ScanCriticalAreas` – die Anwendung führt eine Untersuchung wichtiger Bereiche durch.

    Von Kaspersky Endpoint Security untersuchte wichtige Bereiche

    - /lib/systemd
    - /lib/udev
    - /lib/dbus-1.0
    - /usr/local/lib/systemd/user
    - /usr/share/dbus-1
    - /usr/share/gdm/autostart
    - /usr/share/gnome/autostart
    - /var/spool/at
    - /var/spool/at/spool
    - /var/spool/anacron
    - /var/spool/cron
    - /boot

- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

Sie können mehrere, durch Leerzeichen getrennte Aktionen angeben.

> Wenn Sie das Argument `Skip` angegeben haben, müssen Sie keine weiteren Argumente hinzufügen. Das Argument `Skip` kann nur alleinstehend verwendet werden.

Verwaltung der Ausführungsprävention

Die „Ausführungsprävention“ ermöglicht das Starten ausführbarer Dateien und Skripte sowie das Öffnen von Dateien in Office-Formaten. Die Ausführungsverhinderung verwaltet den Benutzerzugriff auf Dateien mit Ausführungsverhinderungsregeln.

Die Ausführungsprävention für Objekte umfasst die folgenden Aufgaben:

- *Ausführungsprävention für Objekte (EDR Expert (on-premises))* (`KATAEDR_Prevention`)
- *Ausführungsprävention für Objekte (EDR Expert (cloud))* (`EDRExpertCloud_Prevention`)
- *Ausführungsprävention für Objekte (EDR Optimum)* (`EDRO_Prevention`)

Standardmäßig werden Aufgaben der *Ausführungsprävention für Objekte* nicht gestartet. Wenn Sie mindestens eine Regel zur Ausführungsprävention hinzugefügt haben, startet das Programm die Aufgabe.

Um die Liste der Regeln zur Ausführungsprävention für Objekte anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control [-T] --get-prevention-state [--kata|cxdr|edro]
```

wobei:

`--kata`: Liste der Regeln zur Ausführungsprävention für Objekte der Komponente EDR Expert (on-premise)

`--cxdr`: Liste der Regeln zur Ausführungsprävention für Objekte der Komponente EDR Expert (cloud)

`--edro`: Liste der Regeln zur Ausführungsprävention für Objekte der Komponente EDR Optimum

Konfiguration der KUMA-Integration

Über die Befehlszeile können Sie die Integration der Anwendung Kaspersky Endpoint Security mit Kaspersky Unified Monitoring and Analysis Platform mithilfe der vordefinierten Aufgabe *Integration mit Kaspersky Unified Monitoring and Analysis Platform* verwalten.

Die Aufgabe *Integration mit Kaspersky Unified Monitoring and Analysis Platform* wird nicht standardmäßig ausgeführt. Sie können diese Aufgabe manuell starten und beenden.

Sie können Einstellungen für die Integration mit Kaspersky Unified Monitoring and Analysis Platform konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe ändern.

Mithilfe von Befehlen zur Verwaltung der Einstellungen für die Integration mit Kaspersky Unified Monitoring and Analysis Platform können Sie die Zertifikate verwalten, die für die Verbindung zu den KUMA-Servern verwendet werden.

Aufgabe zur Integration mit Kaspersky Unified Monitoring and Analysis Platform

Die folgende Tabelle beschreibt alle verfügbaren Einstellungen und Standardwerte für alle Einstellungen, die Sie für die Aufgabe „Integration mit Kaspersky Unified Monitoring and Analysis Platform“ (`KUMA`) festlegen können.

Parameter	Description	Wert
`UseTls`	Aktivieren und Deaktivieren der Überprüfung des Serverzertifikats, um die Verbindung zum KUMA-Server zusätzlich abzusichern.	`Yes` – Zertifikat verwenden, um die Verbindung zum KUMA-Server zusätzlich abzusichern. `No` (Standardwert) – kein Zertifikat verwenden, um die Verbindung zum KUMA-Server abzusichern.
`UseClientCertificate`	Aktivieren und Deaktivieren der Zwei-Wege-Authentifizierung, um die Verbindung zum KUMA-Server zusätzlich abzusichern. Wenn die Überprüfung des Client-Zertifikats auf der Seite des KUMA-Servers aktiviert ist, müssen Sie die Verwendung des Client-Zertifikats aktivieren und das Client-Zertifikat hinzufügen, bevor Sie die Aufgabe "Integration mit Kaspersky Unified Monitoring and Analysis Platform" ausführen.	`Yes` – Zwei-Wege-Authentifizierung verwenden, um die Verbindung zum KUMA-Server zusätzlich abzusichern. `No` (Standardwert) – Zwei-Wege-Authentifizierung nicht verwenden.
`ConnectionTimeout`	Die maximale Wartezeit auf eine Verbindung mit dem KUMA-Server in Sekunden.	Der Standardwert ist: `5`.
Der Abschnitt **[Servers.item_#]** enthält die Parameter des KUMA-Servers.		
`ServerAddress`	Adresse des KUMA-Servers. Sie können die IP-Adresse (IPv4 oder IPv6) oder den vollqualifizierten Domänennamen (FQDN) des Servers angeben. Wenn Sie den Parameter `UseTls=Yes` festgelegt haben, müssen Sie den vollständig qualifizierten Domänennamen (FQDN) des Servers aus dem Zertifikat angeben, das Sie beim Erwerb Ihrer Lizenz zur Verwendung von KUMA erhalten haben.	Der Standardwert ist: `127.0.0.1`.
`ServerPort`	Port für die Verbindung zum KUMA-Server.	Der Standardwert ist: `443`.
`ServerProtocol`	Protokoll für die Verbindung zum KUMA-Server.	`tcp` (Standardwert) – TCP-Protokoll verwenden, um eine Verbindung zum KUMA-Server herzustellen. `HTTPWithCompression` — HTTP-Protokoll mit Ereigniskomprimierung verwenden, um eine Verbindung zum KUMA-Server herzustellen. `udp` – UDP-Protokoll verwenden, um eine Verbindung zum KUMA-Server herzustellen. Wenn das UDP-Protokoll ausgewählt ist, wird die Verwendung von Zertifikaten zum Schutz der Verbindung nicht unterstützt (die Werte der Einstellungen `UseTls`, `UseClientCertificate` und `ConnectionTimeout` werden ignoriert), und es gibt keine Ereignisse zur Verbindung mit dem KUMA-Server.
Der Abschnitt **[KumaTransferSettings]** enthält Einstellungen für die Übertragung von Ereignissen an den KUMA-Server.		
`EventTransferTimeMax`	Maximale Verzögerung beim Senden von Ereignissen an den KUMA-Server in Sekunden.	Der Standardwert ist: `30`.

Zertifikate für die Verbindung mit dem KUMA-Server verwalten

Wenn UDP-Protokoll ausgewählt ist, wird die Verwendung von Zertifikaten für eine sichere Verbindung nicht unterstützt.

Zur Verwaltung der Zertifikate sind Benutzerrechte mit der Rolle Administrator erforderlich.

Sie können Befehle verwenden, um die Zertifikate zu verwalten, die für die Verbindung mit dem KUMA-Server verwendet werden. Mit Zertifikaten können Sie Folgendes tun:

- 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 [-M] --add-kuma-server-certificate <path to the file>
```

wobei `<path to the file>` der Pfad zur Datei ist, die das Serverzertifikat im DER- oder PEM-Format enthält.

Um ein Client-Zertifikat hinzuzufügen oder zu ersetzen:

1. Führen Sie den folgenden Befehl aus:

   ```
   kesl-control [-M] --add-kuma-client-certificate <path to the file>
   ```

   wobei `<path to the file>` der Pfad zum Crypto-Container (PFX-Archiv) ist, der das Client-Zertifikat und den privaten Schlüssel enthält.

2. Geben Sie das Kennwort für den Crypto-Container ein

Das Client-Zertifikat wird verwendet, um die Verbindung zum KUMA-Server zusätzlich abzusichern, wenn die Überprüfung des Client-Zertifikats in den Einstellungen des KUMA-Servers aktiviert ist und in den Einstellungen der Aufgabe *„Integration mit Kaspersky Unified Monitoring and Analysis Platform“* die Einstellung `UseClientCertificate` auf `yes` festgelegt ist.

Um Informationen zum Zertifikat anzuzeigen, führen Sie den folgenden Befehl aus:

- für das Serverzertifikat:

  ```
  kesl-control [-M] --query-kuma-server-certificate
  ```

- für das Client-Zertifikat:

  ```
  kesl-control [-M] --query-kuma-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 [-M] --remove-kuma-server-certificate
```

Um das Client-Zertifikat zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control [-M] --remove-kuma-client-certificate
```

Allgemeine Einstellungen

In der Verwaltungskonsole können Sie in den Eigenschaften der Richtlinie (**Allgemeine Einstellungen**) allgemeine Programmeinstellungen verwalten, die den Betrieb des Programms insgesamt sowie den Betrieb einzelner Funktionen festlegen.

Allgemeine Anwendungseinstellungen

In der folgenden Tabelle werden allgemeine Programmeinstellungen beschrieben, welche die Funktionsweise des Programms als Ganzes und die Funktionsweise einzelner Funktionen steuern.

Einstellung	Description	Werte
`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. Nach der Änderung dieser Einstellung ist ein Neustart der App erforderlich.	Standardmäßig ist das Standardverzeichnis der Sar Konfigurationsdatei angegeben. Standardwert: /etc/samba/smb.conf
`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. Nach der Änderung dieser Einstellung ist ein Neustart der App erforderlich.	Standardmäßig ist das Standardverzeichnis der NFS Konfigurationsdatei angegeben. Standardwert: /etc/exports
`TraceFolder`	Verzeichnis, in dem die Protokolldateien der Anwendung gespeichert sind. Nach der Änderung dieser Einstellung ist ein Neustart der App erforderlich.	Standardwert: /var/log/kaspersky/kesl. Für den Zugriff auf das Standardverzeichnis zum Sp von Protokolldateien sind Root-Rechte erforderlich. ein anderes Verzeichnis angeben, stellen Sie sicher, root Lese- und Schreibberechtigungen für dieses V hat (Berechtigungen `700` oder `rwx--------`).
`TraceLevel`	Aktiviert die Anwendungsprotokollierung und den Detaillierungsgrad der Protokolldateien. Diese Einstellung aktiviert nur die Erstellung von Protokolldateien des Programms. Um Protokolldateien für die grafische Benutzeroberfläche und das Befehlszeilen-Dienstprogramm kesl-control zu erstellen, müssen Sie die Umgebungsvariable LFS_ENABLE_ALL_COMPONENTS_LOGGING festlegen.	`Detailed` – Detaillierte Protokolldatei des Program erstellen. `MediumDetailed` – Protokolldatei des Programms die Info-Meldungen und Fehlermeldungen enthält. `NotDetailed` – Protokolldatei des Programms erst Fehlermeldungen enthält. `None` (Standardwert) – Keine Protokolldatei des Pro erstellen.
`TraceMaxFileCount`	Gibt die Maximalanzahl der Protokolldateien der App an. Nach der Änderung dieser Einstellung ist ein Neustart der App erforderlich.	1 bis 10000 Standardwert: 10.
`TraceMaxFileSize`	Legt die maximale Größe der Protokolldatei der App fest (in Megabyte). Nach der Änderung dieser Einstellung ist ein Neustart der App erforderlich.	1 bis 1000 Standardwert: 500.

Einstellung	Description	Werte
`WdTraceLevel`	Aktiviert die Watchdog-Server-Protokollierung und den Detaillierungsgrad der Protokolldateien.	`Detailed` – Detaillierte Protokolldatei des Watchd erstellen. `MediumDetailed` – Protokolldatei des Watchdog- erstellen, die Info-Meldungen und Fehlermeldungen `NotDetailed` – Protokolldatei des Watchdog-Serv erstellen, die Fehlermeldungen enthält. `None` – Keine Protokolldatei des Watchdog-Server `Product` (Standardwert) – Wert auf den Wert `Tra` festlegen.
`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. Dieser Parameter gilt nur für Betriebssysteme, von denen die fanotify-Technologie nicht unterstützt wird. Nachdem Sie den Wert für diesen Parameter geändert haben, muss die Aufgabe „Schutz vor bedrohlichen Dateien“ neu gestartet werden.	4096 bis 33554432 Standardwert: 16384.
`DetectOtherObjects`	Aktiviert die Erkennung legitimer Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können.	`Yes` – Aktiviert die Erkennung legaler Programme, c Angreifern zur Beschädigung von Geräten oder Dat ausgenutzt werden können. `No` (Standardwert) – Deaktiviert die Erkennung lega Programme, die von Angreifern zur Beschädigung v oder Daten ausgenutzt werden können.
`NamespaceMonitoring`	Aktiviert die Untersuchung von Namespaces und Containern. Die Anwendung prüft keine Namensräume und Container, es sei denn, auf dem Betriebssystem sind Komponenten für die Arbeit mit Containern und Namensräumen installiert.	`Yes` (Standardwert) aktiviert die Untersuchung von Namensräumen und Containern. `No` deaktiviert die Untersuchung von Namensräume Containern.
`FileBlockDuringScan`	Aktivieren des Modus des Interceptors von Dateioperationen mit Blockieren des Zugriffs auf Dateien während der Untersuchung. Der Modus zum Abfangen von Dateioperationen wirkt sich auf die Komponenten Schutz vor bedrohlichen Dateien und Gerätekontrolle, die Aktion Ausführungsprävention für Objekte und die Aufgabe Untersuchung von Wechseldatenträgern aus.	`Yes` (Standardwert) — Zugriff auf Dateien für die D Untersuchung blockieren. `No` – Zugriff auf Dateien während des Untersuchun blockieren. Der Zugriff auf eine beliebige Datei ist er Überprüfung erfolgt im asynchronen Modus. Die Ko Schutz vor bedrohlichen Dateien, Gerätekontrolle u Ausführungsprävention sowie die Aufgabe Untersu Wechseldatenträgern werden jedoch unabhängig v ausgewählten Betriebsmodus im Modus „Informiere ausgeführt. Diese Art des Abfangens von Dateivorg sich weniger stark auf die Systemleistung aus. Allerd werden in diesem Fall in Dateien gefundene Bedrohu weder desinfiziert noch gelöscht. Dies kann vorkom es dem mit dieser Datei verknüpften Prozess währe Untersuchung gelingt, die Datei umzubenennen, bev Programm eine Entscheidung über den Status diese treffen kann. Sie können die Aufgabe Schadsoftwar Untersuchung ausführen, um solche Bedrohungen s verarbeiten.

Einstellung	Description	Werte
`UseKSN`	Verwendung von Kaspersky Security Network während der Anwendungsausführung konfigurieren	`Basic` – Verwendung von Kaspersky Security Netw Standard-Modus aktivieren. `Extended` – Verwendung von Kaspersky Security N erweiterten Modus aktivieren. `No` (Standardwert) – Kaspersky Security Network r verwenden.
`CloudMode`	Aktivieren des Cloud-Modus der Anwendung. 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 Anwendung im Standard-Modus verwendet wird.	`Yes` (Standardwert) — Betriebsmodus aktivieren, in Kaspersky Endpoint Security eine schlankere Versic Malware-Datenbanken verwendet. `No` (Standardwert) – Vollversion der Malware-Date verwenden. Der Cloud-Modus wird automatisch deaktiviert, KSN deaktiviert ist.
`UseMDR`	Aktivieren der Komponente "Managed Detection and Response" für die Integration mit Kaspersky Managed Detection and Response. Wenn Sie die MDR-Komponente aktivieren und Kaspersky Security Network deaktiviert ist oder im Standardmodus ausgeführt wird, erscheint eine Fehlermeldung und die MDR-Komponente wird nicht aktiviert. Um die MDR-Komponente zu aktivieren, muss Kaspersky Security Center im erweiterten Modus aktiviert werden. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`Yes` – Komponente „Managed Detection and Respo aktivieren. `No` (Standardwert) – Komponente „Managed Detec Response“ deaktivieren.
`UseEdrOptimum`	Aktivieren der Komponente "EDR Optimum" für die Integration mit Kaspersky Endpoint Detection and Response Optimum. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`Yes` – Komponente „EDR Optimum“ aktivieren. `No` (Standardwert) – Komponente „EDR Optimum“ deaktivieren.
`UseProxy`	Aktiviert die Verwendung eines Proxyservers durch Komponenten von Kaspersky Endpoint Security. Ein Proxyserver kann für folgende Vorgänge verwenden: für den Zugriff auf die Aktivierungsserver von Kaspersky, auf die Update-Quellen für Datenbanken und Module der Anwendung und auf Kaspersky Security Network sowie für die Untersuchung von Website-Zertifikaten mit dem Schutz vor Web-Bedrohungen. Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, wird die Verwendung eines Proxyservers für die Verbindung mit Kaspersky Security Network, der SVM und dem Integrationsserver nicht unterstützt.	`Yes`: Nutzung eines Proxyservers aktivieren. `No` (Standardwert) – Nutzung eines Proxy-Servers deaktivieren.

Einstellung	Description	Werte
`ProxyServer`	Adresse des Proxyservers, der für die Internetverbindung verwendet wird 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 verwendet eine unsichere Verbindung und das Benutzerkonto ist möglicherweise kompromittiert.	Adresse des Proxyservers in einem der folgenden F • `[<connection protocol>://]<address o proxy server>:<port>`, wenn für die Verbind mit dem Proxyserver keine Authentifizierung erforderlich ist; • `[<connection protocol>://][<user name [<password>]@]<address of the proxy s <port>`, wenn für die Verbindung mit dem Prox eine Authentifizierung erforderlich ist. Geben S IPv6-Adresse in eckigen Klammern ein. Das Herstellen einer Verbindung mit dem Proxyse über das HTTPS-Protokoll wird nicht unterstützt
`ProxyBypass`	Liste mit Adressen, für deren Verbindung kein Proxyserver verwendet wird.	Die Adresse wird im Format `<address>[:<port>]` Um Adressen anzugeben, können Sie Masken (Symb Kommentare nach dem Symbol `\` verwenden.
`ProxyBypassEdr`	Ob beim Herstellen einer Verbindung mit Integrationsservern für Kaspersky Endpoint Detection and Response Expert (on-premise) ein Proxyserver verwendet wird. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`Yes`, um bei der Verbindung mit Integrationsserverr Kaspersky Endpoint Detection and Response Exper premise) keinen Proxyserver zu verwenden. `No` (Standardwert), um bei der Verbindung mit Integrationsservern für Kaspersky Endpoint Detect Response Expert (on-premise) einen Proxyserver zu verwenden.
`ProxyBypassNdr`	Verwendung des Proxyservers bei einer Verbindung mit Servern, welche die Integration mit Kaspersky Network Detection and Response (KATA) gewährleisten. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`Yes` – Kein Proxyserver für die Verbindung mit Serv verwenden, welche die Integration mit Kaspersky Ne Detection and Response (KATA) gewährleisten. `No` (Standardwert) – Proxyserver für die Verbindun Servern verwenden, welche die Integration mit Kasp Netzwork Detection and Response (KATA) gewährle
`ProxyBypassSandbox`	Verwendung des Proxyservers bei einer Verbindung mit Servern, welche die Integration mit Sandbox gewährleisten. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`Yes` – Kein Proxyserver für die Verbindung mit Serv verwenden, welche die Integration mit Sandbox gew `No` (Standardwert) – Proxyserver für die Verbindun Servern verwenden, welche die Integration mit Sanc gewährleisten.
`MaxEventsNumber`	Maximale Anzahl von Ereignissen, die von der App gespeichert werden. Wenn die angegebene Anzahl von Ereignissen übertroffen wird, lösch die Anwendung die ältesten Ereignisse.	Standardwert: 500000. Wenn der Wert auf "0" gesetzt ist, werden keine neu Ereignisse gespeichert und alle alten gelöscht.
`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 oder der Rolle kesladmin starten kann, nicht beschränkt.	0 bis 100000 0 – Ein nicht berechtigter Benutzer kann Aufgaben benutzerdefinierten Untersuchung nicht starten. Standardwert: 100.
`UseSyslog`	Aktivieren der Aufzeichnung von Anwendungsereignissen in syslog. Für den Zugriff auf syslog sind Root-Rechte erforderlich.	`Yes` – Protokollieren von Ereignissen im syslog aktiv `No` (Standardwert) – Protokollieren von Ereignissen deaktivieren.

Einstellung	Description	Werte
`EventsStoragePath`	Pfad zur Hauptdatei der Datenbank des Ereignisprotokolls. Für den Zugriff auf die Standarddatenbank mit Ereignissen sind Root-Rechte erforderlich.	Standardwert: `/var/opt/kaspersky/kesl/private/storage/`
`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 Remote-Verzeichnisse, Gerät über SMB- oder NFS-Protokolle gemountet s vom Modul zum Abfangen von Dateioperationen ausgeschlossen. `Mounted:NFS` – Alle Remote-Verzeichnisse, die auf über NFS-Protokolle gemountet sind, werden vom M Abfangen von Dateioperationen ausgeschlossen. `Mounted:SMB` – Alle Remote-Verzeichnisse, die auf über SMB-Protokolle gemountet sind, werden vom Abfangen von Dateioperationen ausgeschlossen. `Mounted:<file system type>`: Alle eingehängte Verzeichnisse mit dem angegebenen Dateisystemty Abfangen von Dateioperationen ausschließen. `/mnt` — Objekte im Mountpunkt /mnt (einschließlich Unterverzeichnissen) vom Abfangen von Dateioperat ausschließen. Dieses Verzeichnis wird als temporäre Mountpunkt für Wechseldatenträger verwendet. `<path that contains the /mnt/user*|/mnt/**/user_share>`: Objekte in Einhängepunkten, deren Namen die angegebene Ma enthalten, vom Abfangen von Dateioperationen aus
`MemScanExcludedProgramPath.item_#`	Prozess-Speicher von der Untersuchung ausschließen. Der Arbeitsspeicher des angegebenen Prozesses wird von der Anwendung nicht untersucht.	`<full path to process>` — Objekte im angegeb Verzeichnis von der Untersuchung ausschließen. Be Angabe des Pfades können Masken verwendet wer
`PowerSaveMode`	Abbrechen geplanter Aufgaben auf einem, das im Akkubetrieb läuft.	`Yes` (Standardwert) – Geplante Aufgaben auf einer das im Akkubetrieb läuft, überspringen. `No` – Geplante Aufgaben auf einem Gerät unabhäng Stromquelle (Netz oder Akku) planmäßig ausführen.
`UseOnDemandCPULimit`	Aktiviert die Begrenzung der CPU-Auslastung für Aufgaben vom Typ *ODS*, *ContainerScan* und *InventoryScan*.	`Yes` – Aktiviert die Begrenzung der Nutzung von CP Ressourcen für die Aufgabentypen *ODS*, *Container* *InventoryScan*. `No` (Standardwert) – Deaktiviert die Begrenzung de von CPU-Ressourcen für Aufgaben.
`OnDemandCPULimit`	Maximale Auslastung aller Prozessorkerne (in Prozent) bei der Ausführung von Aufgaben vom Typ *ODS*, *ContainerScan* und *InventoryScan*.	Eine Ganzzahl zwischen 10 und 100. Standardwert: 100.
`BackupSizeLimit`	Maximale Backup-Größe (in Megabyte) Wenn die maximale Größe des Backups erreicht ist, löscht die Anwendung die ältesten Backup-Dateien. Um die Begrenzung der Backup-Größe aufzuheben, geben Sie den Wert 0 an.	0 – 4000 0 – Die Größe des Backups ist nicht begrenzt. Standardwert: 0.
`BackupDaysToLive`	Speicherzeit von Objekten im Backup (in Tagen) Nach Ablauf des angegebenen Zeitraums löscht die Anwendung die ältesten Backup-Dateien. Um die Begrenzung der Speicherzeit von Objekten im Backup aufzuheben, geben Sie den Wert 0 an.	0 – 10000 0 – Die Speicherzeit von Objekten im Backup ist nic begrenzt. Standardwert: 30.

Einstellung	Description	Werte
`QuarantineSizeLimit`	Maximale Größe der Quarantäne (in Megabyte). Wenn die maximale Größe des Quarantäne-Speichers erreicht ist, löscht die Anwendung die ältesten Objekte. Um die Begrenzung der Quarantäne-Größe aufzuheben, geben Sie den Wert 0 an. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	0 – 999999 0 – Die Größe der Quarantäne ist nicht begrenzt. Der Standardwert beträgt 200, wenn die App im St Modus verwendet wird, und 100, wenn die App im Li Modus verwendet wird.
`QuarantineFillingNotification`	Füllstand der Quarantäne in Prozent, bei dessen Erreichen eine Ereignis über mangelnden Quarantäne-Speicher generiert werden soll. Um das Generieren von Ereignissen über den Quarantäne-Füllstand zu deaktivieren, geben Sie den Wert 0 ein. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	0 – 100 0 – Das Generieren von Ereignissen über den Quara Füllstand ist deaktiviert. Standardwert: 90.
`QuarantineBackupFolder`	Pfad zum Verzeichnis, in dem die Backup-Kopien von Dateien und Dateien, die in die Quarantäne verschoben wurden, gespeichert werden. Sie können das Standardverzeichnis ändern. Wenn das angegebene Verzeichnis nicht existiert oder nicht verfügbar ist, verwendet die Anwendung das Standardverzeichnis. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU. Die Einstellung `BackupFolder` wird verwendet.	Standardwert: `/var/opt/kaspersky/kesl/common/objects-b` Für den Zugriff auf das Standardverzeichnis sind Rechte erforderlich.
`BackupFolder`	Pfad zum Verzeichnis Backup. Sie können das Standardverzeichnis ändern. Wenn das angegebene Verzeichnis nicht existiert oder nicht verfügbar ist, verwendet die Anwendung das Standardverzeichnis.	Der Standardwert ist `/var/opt/kaspersky/kesl/common/objects-b` Für den Zugriff auf das Standardverzeichnis für Backup sind Root-Rechte erforderlich.
`ShowPopUpNotifications`	Aktivieren der Anzeigen von Pop-up-Benachrichtigungen in der grafischen Benutzeroberfläche.	`Yes` (Standardwert) – In der grafischen Benutzerob werden Pop-up-Benachrichtigungen angezeigt. `No` – In der grafischen Benutzeroberfläche werden up-Benachrichtigungen angezeigt.
`InterceptorMode`	Der von Kaspersky Endpoint Security verwendete Mechanismus zum Abfangen von Systemereignissen: Der Parameter wird nur auf Geräten angewendet, deren Betriebssystem die fanotify-Technologie unterstützt. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`UseFanotify` (Standardwert) – fanotify-Technolo Abfangen von Systemereignissen verwenden. `UseUpdatableKernelModule` – Aktualisierbares K Modul zum Abfangen von Systemereignissen verwe

Einstellung	Description	Werte
`InterceptorFallbackStrategy`	Von der Anwendung ausgeführte Aktion, wenn der Start des aktualisierbaren Kernel-Moduls fehlschlägt. Der Parameter wird nur auf Geräten angewendet, deren Betriebssystem die fanotify-Technologie unterstützt.	`FallbackToFanotify` (Standardwert) – Zur Verwe fanotify-Technologie zum Abfangen von Systemere übergehen. `FallbackToLimitedMode` – Systemereignisse nicl abfangen. Wenn das Abfangen von Systemereigniss Anwendung nicht verwendet wird, findet keine Dateiuntersuchung in Echtzeit statt. Dies reduziert Schutzstufe des Geräts.
`InterceptorApplyStrategy`	Wenn die Anwendung zur Verwendung des aktualisierbaren Kernel-Moduls übergeht, ist zum Starten des Moduls ein Neustart der Anwendung erforderlich. Dieser Parameter gibt an, ob die Anwendung automatisch neu gestartet wird, oder ob ein manueller Neustart der Anwendung erforderlich ist. Der Parameter wird nur auf Geräten angewendet, deren Betriebssystem die fanotify-Technologie unterstützt.	`RestartServiceAutomatically` (empfohlener W Anwendung automatisch neu starten, um das aktua Kernel-Modul zu starten. Wir empfehlen, diese Einst verwenden. `RestartServiceManually` (Standard) startet das aktualisierbare Kernel-Modul, nachdem das Program Benutzer manuell neu gestartet wurde.
`SystemEventsTransmission`	Aktivierung der Übertragung von Informationen über Ereignisse aus Drittanbieter-Apps (die keine Kaspersky-Lösungen sind). Wenn diese Einstellung aktiviert ist, sendet Kaspersky Endpoint Security zusätzlich zu eigenen Ereignissen auch systemd-journald-Ereignisse von Drittanbieter-Apps an das Ereignisprotokoll der App. Für den Zugriff auf systemd-journald sind Root-Rechte erforderlich.	`Yes` – Übertragung von Informationen über system Ereignisse von Drittanbieter-Apps an das Ereignispr App aktivieren. `No` (Standardwert) – Übertragung von Informatione systemd-journald-Ereignisse von Drittanbieter-App Ereignisprotokoll der App deaktivieren.
`UrgentUpdateRestartEnabled`	Das Programm beim Erhalt kritischer Updates automatisch neu starten.	`Yes` – App beim Empfang kritischer Updates autom starten. `No` (Standardwert), um die App beim Empfang kritis Updates nicht neu zu starten. Wenn innerhalb von 24 Stunden nach der Installatio Programms beim ersten Update der Datenbanken u kritische Updates empfangen werden, wird das Prog unabhängig vom Wert des Parameters `UrgentUpdateRestartEnabled` automatisch neu
`CoreDumps`	Aktiviert die Erstellung einer Dump-Datei im Falle eines Absturzes der Anwendung.	`Yes`, um eine Dump-Datei zu erstellen, wenn die App `No` (Standardwert), um keine Dump-Datei zu erstell App abstürzt.
`CoreDumpsPath`	Pfad zum Verzeichnis, in dem die Dump-Dateien gespeichert werden.	Standardwert: `/var/opt/kaspersky/kesl/common/dumps` Für den Zugriff auf das Standardverzeichnis zum Speichern von Dump-Dateien sind Root-Rechte erforderlich.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Aufgabenzeitplan

In der folgenden Tabelle werden die Einstellungen des Aufgabenzeitplans beschrieben, die Sie für alle Programmaufgaben verwalten können.

Einstellungen des Zeitplans für den Aufgabenstart

Parameter	Description
`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 Anwendung starten. • `BR` – Aufgabe nach dem Update der Anwendungsdatenbanken starten.
`StartTime`	Datum und Uhrzeit des Aufgabenstarts. Das Format dieser Einstellung hängt von `RuleType` ab. Mögliche Werte: • `<year>`: 1970 bis 2099 • `<month>`: JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC. • `<day of the month>`: 1 bis 31 • `<day of the week>`: Mon, Tue, Wed, Thu, Fri, Sat, Sun. • `<hh>`: 0 bis 23 • `<mm>`: 0 bis 59 • `<ss>`: 0 bis 59 • `<interval between runs (in days)>`: 0 bis 364 • `<interval between runs (in hours)>`: 0 bis 23 • `<interval between runs (in minutes)>`: 0 bis 59
`RandomInterval`	Führen Sie die Aufgabe auf den Computern zu einem zufälligen Zeitpunkt innerhalb eines bestimmten Zeitintervalls (von 0 bis zum angegebenen Wert) aus. Dadurch wird vermieden, dass mehrere Aufgaben gleichzeitig gestartet werden. Standardwert: 99 Minuten. Zulässige Werte: 0 – 999.

Parameter	Description
`RunMissedStartRules`	Start einer übersprungenen Aufgabe nach dem Starten der App. • `Yes` (Standardwert) bedeutet, dass die Ausführung einer verpassten Aufgabe aktiviert ist. Wenn das Programm angehalten oder der Computer ausgeschaltet wird, während eine geplante Aufgabe ausgeführt wird, startet Kaspersky Endpoint Security diese Aufgabe sofort nach dem Start des Programms. So können Sie sicherstellen, dass kritische Aufgaben niemals verpasst werden. • `No` bedeutet, dass die Ausführung einer verpassten Aufgabe deaktiviert ist. Wenn das Programm angehalten oder der Computer ausgeschaltet wird, während eine geplante Aufgabe ausgeführt wird, überspringt das Programm diese Aufgabe. Dadurch wird eine zusätzliche Belastung beim Start des Programms vermieden.
`UseWorkingTimeout`	Stoppen der Aufgabe, wenn die durch den Parameter `WorkingTimeout` angegebene maximale Ausführungszeit der Aufgabe erreicht ist. Die Aufgabe wird auch dann gestoppt, wenn sie noch nicht abgeschlossen ist. Der nächste Aufgabenstart wird entsprechend des Zeitplans durchgeführt. • `Yes` – Stoppt die Aufgabe, wenn deren maximale Ausführungszeit erreicht wurde. • `No` (Standardwert) – Stoppt die Aufgabe nicht, wenn deren maximale Ausführungszeit erreicht wurde.
`WorkingTimeout`	Die maximale Ausführungszeit der Aufgabe (in Minuten). Beim Erreichen dieses Wertes wird die Ausführung der Aufgabe von der Anwendung gestoppt, wenn der Wert des Parameters `UseWorkingTimeout=Yes` festgelegt ist. Standardwert: 120 Minuten. Zulässige Werte: 1 – 999.

Einstellungen für Proxyserver

In der Befehlszeile können Sie die Verwendung des Proxyservers durch die Anwendungskomponenten anhand der Parameter `UseProxy`, `ProxyServer`, `ProxyBypass`, `ProxyBypassEdr`, `ProxyBypassNdr` und `ProxyBypassSandbox` aus den allgemeinen Anwendungseinstellungen konfigurieren.

Sie können die Werte der Einstellungen mithilfe von Befehlszeilenschaltern oder einer Konfigurationsdatei ändern, die alle allgemeinen Programmeinstellungen enthält.

Der Parameter `UseProxy` kann folgende Werte annehmen:

- `Yes` aktiviert die Nutzung eines Proxyservers.
- `No` deaktiviert den Proxyserver.

Mit der Einstellung ProxyServer können die Proxyserver-Einstellungen im Format `<connection protocol>://[<user>[:<password>]@]<proxy server address>:<port number>` angegeben werden, wobei gilt:

- `<user>` ist der Benutzername für die Authentifizierung am Proxyserver.
- `<password>` ist das Benutzerkennwort für die Authentifizierung am Proxyserver.
- `<proxy server address>` ist die IP-Adresse oder der Domänenname des Proxyservers.
- `<port number>` ist die Portnummer des Proxyservers.

Das Herstellen einer Verbindung mit dem Proxyserver über das HTTPS-Protokoll wird nicht unterstützt.

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 verwendet eine unsichere Verbindung und das Benutzerkonto ist möglicherweise kompromittiert.

Mit dem Parameter `ProxyBypass` können Sie eine Liste von Adressen angeben, für deren Verbindung kein Proxyserver verwendet wird. Die Adresse wird im Format `<address>[:<port number>]` angegeben. Zur Angabe von Adressen können Sie Platzhalter (`*`-Symbole) und Kommentare (nach einem "\"-Symbol) verwenden.

Die folgenden Parameter erlauben die Konfiguration der Verwendung eines Proxyservers durch die Komponenten EDR Expert (on-premise), NDR (KATA) und Sandbox, welche die Integration mit Detection and Response-Lösungen gewährleisten:

- Der Parameter `ProxyBypassEdr` erlaubt das Aktivieren und Deaktivieren der Verwendung eines Proxyservers bei einer Verbindung zu Servern, welche die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA) gewährleisten.
- Der Parameter `ProxyBypassNdr` erlaubt das Aktivieren und Deaktivieren der Verwendung eines Proxyservers bei einer Verbindung zu Servern, welche die Integration mit Kaspersky Network Detection and Response (KATA) gewährleisten.
- Der Parameter `ProxyBypassSandbox` erlaubt das Aktivieren und Deaktivieren der Verwendung eines Proxyservers bei einer Verbindung zu Servern, welche die Interaktion mit der Sandbox gewährleisten.

Die Parameter können die folgenden Werte annehmen:

- `Yes` aktiviert die Nutzung eines Proxyservers.
- `No` deaktiviert den Proxyserver.

Backup-Einstellungen konfigurieren

Über die Befehlszeile können Sie die Backup-Einstellungen mithilfe der Optionen `BackupDaysToLive,`, `BackupSizeLimit` und `QuarantineBackupFolder` in den allgemeinen Anwendungseinstellungen konfigurieren.

Sie können die Werte der Einstellungen mithilfe von Befehlszeilenschaltern oder einer Konfigurationsdatei ändern, die alle allgemeinen Programmeinstellungen enthält.

Backup-Einstellungen

Parameter	Description	Wert
`BackupDaysToLive`	Speicherzeit von Objekten im Backup (in Tagen) Nach Ablauf des angegebenen Zeitraums löscht die Anwendung die ältesten Backup-Dateien. Um die Begrenzung der Speicherzeit von Objekten im Backup aufzuheben, geben Sie den Wert 0 an.	0 – 10000 0 – Die Speicherzeit von Objekten im Backup ist nicht begrenzt. Standardwert: 30.
`BackupSizeLimit`	Maximale Backup-Größe (in Megabyte) Wenn die maximale Größe des Backups erreicht ist, löscht die Anwendung die ältesten Backup-Dateien. Um die Begrenzung der Backup-Größe aufzuheben, geben Sie den Wert 0 an.	0 – 4000 0 – Die Größe des Backups ist nicht begrenzt. Standardwert: 0.

Parameter	Description	Wert
`QuarantineBackupFolder`	Pfad zum Verzeichnis, in dem die Backup-Kopien von Dateien und Dateien, die in die Quarantäne verschoben wurden, gespeichert werden. Sie können das Standardverzeichnis ändern. Wenn das angegebene Verzeichnis nicht existiert oder nicht verfügbar ist, verwendet die Anwendung das Standardverzeichnis. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU. Die Einstellung `BackupFolder` wird verwendet.	Der Standardwert ist `/var/opt/kaspersky/kesl/common/objects-backup/` Für den Zugriff auf das Standardverzeichnis sind Root-Rechte erforderlich.
`BackupFolder`	Pfad zum Verzeichnis Backup. Sie können das Standardverzeichnis ändern. Wenn das angegebene Verzeichnis nicht existiert oder nicht verfügbar ist, verwendet die Anwendung das Standardverzeichnis.	Der Standardwert ist `/var/opt/kaspersky/kesl/common/objects-backup/` Für den Zugriff auf das Standardverzeichnis für das Backup sind Root-Rechte erforderlich.

Einstellungen der Untersuchung des Netzwerkdatenverkehrs

Einstellungen der Untersuchung des Netzwerkdatenverkehrs

Parameter	Description	Werte
`EncryptedConnectionsScan`	Aktiviert oder deaktiviert die Untersuchung von verschlüsselten Verbindungen. Für das FTP-Protokoll ist die Untersuchung verschlüsselter Verbindungen standardmäßig deaktiviert.	`Yes` (Standardwert) – Untersuchung verschlüsselter Verbindungen aktivieren `No` – Untersuchung verschlüsselter Verbindungen deaktivieren Die App entschlüsselt den verschlüsselten Datenverkehr nicht.
`EncryptedConnectionsScanErrorAction`	Legt die Aktion der App fest, die ausgeführt werden soll, wenn auf einer Website ein Fehler bei der Untersuchung der verschlüsselten 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 Anwendung keine zusätzliche Überprüfung durch.	`FullCheck` (Standardwert) – Die Anwendung nutzt das Internet, um die fehlenden Ketten, die zur Überprüfung des Zertifikats erforderlich sind, zu prüfen und herunterzuladen. `LocalCheck` – Die Anwendung nutzt zur Überprüfung des Zertifikats nicht das Internet.
`UntrustedCertificateAction`	Aktion, welche 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 unter `[Exclusions.item_#]` angegeben sind, nicht untersuchen (siehe unten). `No` (Standardwert) – Alle Websites untersuchen

Parameter	Description	Werte
`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.
`NetInterceptorMode`	Modus zum Abfangen des Datenverkehrs in der Kaspersky Endpoint Security. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`UseEBPF` – Zum Abfangen des Datenverkehrs die eBPF-Technologie verwenden. `UseIPTables` (Standardwert) – Zum Abfangen des Datenverkehrs das iptables-Tool verwenden. Um den Modus zum Abfangen des Datenverkehrs zu ändern, muss die Anwendung neu gestartet werden. Während des Neustarts werden bestehende Netzwerkverbindungen unterbrochen.
Der Abschnitt **[Exclusions.item_#]** enthält Domains, die von der Untersuchung ausgeschlossen werden sollen. Die Anwendung untersucht keine Verbindungen, die beim Aufruf bestimmter Domänen hergestellt wurden.		
`DomainName`	Gibt den Domain-Namen an.	Für die Angabe der Domäne können Sie Masken verwenden.
Der Abschnitt **[IncomingEndpointsExclusions.item_#]** enthält Ausnahmen für eingehenden Datenverkehr.		
`RemoteIp`	Die IP-Adresse des Remote-Geräts, von dem der Datenverkehr vom Abfangen ausgeschlossen wird.	
`DestinationPort`	Der Port des geschützten Geräts, zu dem der Datenverkehr von Remote-Geräten vom Abfangen ausgeschlossen wird.	
Der Abschnitt **[OutgoingEndpointsExclusions.item_#]** enthält Ausnahmen für ausgehenden Datenverkehr.		
`RemoteIp`	Die IP-Adresse des Remote-Geräts, zu dem der Datenverkehr vom Abfangen ausgeschlossen wird.	
`DestinationPort`	Der Port des Remote-Geräts, zu dem der Datenverkehr von geschützten Geräten vom Abfangen ausgeschlossen wird.	
Der Abschnitt **[NetworkPorts.item_#]** enthält die Netzwerkports, welche die Anwendung überwachen soll.		
`PortName`	Beschreibung des Netzwerkports.	
`Port`	Nummern der Netzwerkports, welche die App überwachen soll.	`1 – 65535`. Der Standardwert ist nicht angegeben.

Globale Ausschlüsse konfigurieren

Über die Befehlszeile können Sie den Ausschluss von Mountpunkten mithilfe des Parameters `ExcludedMountPoint.item_#` in den allgemeinen Anwendungseinstellungen konfigurieren.

Sie können den Wert der Einstellung mithilfe von Befehlszeilenschaltern oder einer Konfigurationsdatei ändern, die alle allgemeinen Programmeinstellungen enthält.

Der Parameter `ExcludedMountPoint.item_#` kann folgende 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:<file system type>`: Alle eingehängten Verzeichnisse mit dem angegebenen Dateisystemtyp vom Abfangen von Dateioperationen ausschließen.
- `/mnt` — Objekte im Mountpunkt /mnt (einschließlich Unterverzeichnissen) vom Abfangen von Dateioperationen ausschließen. Dieses Verzeichnis wird als temporärer Mountpunkt für Wechseldatenträger verwendet.
- `<path containing the mask /mnt/user* or /mnt/**/user_share>`: Objekte in Einhängepunkten, deren Namen die angegebene Maske enthalten, vom Abfangen von Dateioperationen ausschließen.

Die Mountpunkte müssen genau so angegeben werden, wie sie in der Ausgabe des Befehls `mount` angezeigt werden.

Sie können mehrere Mountpunkte angeben, die Sie von der Untersuchung ausschließen möchten.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Einstellungen für den Kennwortschutz

Sie können die Rechte zur Verwaltung des Programms gewähren oder entziehen, indem Sie mithilfe von Befehlszeilenoptionen Einstellungen ändern oder eine Konfigurationsdatei bearbeiten.

Einstellungen für den Kennwortschutz

Parameter	Description	Wert
`StopProtection`	Deaktivieren von Schutzkomponenten.	`Yes` erlaubt dem Benutzer, die Aktion auszuführen. `No` verbietet dem Benutzer, eine Aktion auszuführen.
`StopSecurityControl`	Überwachungskomponenten deaktivieren	
`StartProtection`	Aktivieren von Schutzkomponenten	
`StartSecurityControl`	Aktivieren von Kontrollkomponenten	
`ApplicationSettings`	Konfigurieren des Programms	
`ViewReports`	Berichte anzeigen	
`RestoreFromBackup`	Wiederherstellen aus dem Backup	
`RemoveLicenseKey`	Schlüssel löschen	
`AddLicense`	Hinzufügen eines Schlüssels	
`DisablePolicy`	Deaktivieren der Richtlinie für Kaspersky Security Center	

Programmeinstellungen in der Verwaltungskonsole

Sie verwenden eine Richtlinie, um Kaspersky Endpoint Security zu konfigurieren. Ausführliche Informationen über die Programmkomponenten finden Sie in den entsprechenden Unterabschnitten.

Datenbanken-Update

In der Verwaltungskonsole können Sie Datenbanken mithilfe der Aufgabe „Update“ aktualisieren.

Sie können Update-Benutzeraufgaben erstellen und ausführen. Sie können die Update-Einstellungen verwalten, indem Sie die Aufgabeneinstellungen ändern.

In den Eigenschaften der Aufgabe „Update“ können Sie in den Abschnitten **Update-Quellen** und **Einstellungen** die in der folgenden Tabelle aufgeführten Einstellungen verwalten.

Abschnitt "Update-Quellen für die Update-Aufgabe"

Parameter	Description

Update-Quelle	Diese Tabelle enthält eine Liste mit den Quellen für die 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** – Adresse der Update-Quelle:
	  • **Kaspersky-Update-Server**, auf denen Datenbanken-Updates für alle Anwendungen von Kaspersky veröffentlicht werden (Standardwert).
	  • **Kaspersky Security Center** – Kaspersky Security Center Administrationsserver.
	  • Andere, durch einen Benutzer hinzugefügte Quellen im lokalen oder globalen Netzwerk: HTTP-, HTTPS- oder FTP-Server bzw. Verzeichnisse auf Servern im lokalen Netzwerk.
	• **Status** zeigt an, ob die Update-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 **Ändern** klicken.
	Sie können Update-Quellen in der Tabelle hinzufügen, bearbeiten, löschen, nach oben oder nach unten verschieben.

Abschnitt "Einstellungen der Update-Aufgabe"

Parameter	Description
Maximale Wartezeit auf eine Antwort der Update-Quelle (Sek.)	Maximale Wartezeit (in Sekunden), der Anwendung 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 Anwendung von der ausgewählten Quelle nicht beschränkt. Standardwert: 10 Sekunden
Download-Modus für Updates	In dieser Dropdown-Liste können Sie Download-Modus für automatisch installierbare Anwendungsupdates (Autopatches) festlegen: • **Nicht herunterladen**. Wenn dieses Element ausgewählt ist, werden Autopatches nicht automatisch heruntergeladen. • **Nur herunterladen**. Wenn dieses Element ausgewählt ist, werden Autopatches automatisch heruntergeladen, aber nicht auf den Client-Geräten installiert (Standardwert). • **Herunterladen und installieren**. Wenn dieses Element ausgewählt ist, werden Autopatches automatisch heruntergeladen und auf den Client-Geräten installiert. Nach der Installation eines Autopatches wird die Anwendung automatisch neu gestartet.

Geräteschutz vor Bedrohungen

Komponente "Schutz vor bedrohlichen Dateien".

In der Verwaltungskonsole können Sie den Schutz vor bedrohlichen Dateien in den Richtlinieneigenschaften verwalten (**Basisschutz → Schutz vor bedrohlichen Dateien**).

Einstellungen der Komponente „Schutz vor bedrohlichen Dateien"

Parameter	Description
Schutz vor bedrohlichen Dateien aktivieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Komponente zum Schutz vor bedrohlichen Dateien auf allen verwalteten Geräten. Dieses 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 Ändern. • **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.
Aktionen beim Erkennen von Bedrohungen	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster Aktionen beim Erkennen von Bedrohungen geöffnet, in dem Sie die Aktionen konfigurieren können, die die App für erkannte infizierte Objekte ausführt.

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.

Parameter	Description
Name des Bereichs	Name des Untersuchungsbereichs
Path	Der Pfad zu dem zu untersuchenden Verzeichnis.
Status	Der Status gibt an, ob die Anwendung 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 aufgeführt sind. Wenn Sie für ein Unterverzeichnis Sicherheitseinstellungen anpassen möchten, die sich von den Sicherheitseinstellungen des übergeordneten Verzeichnisses unterscheiden, 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 aufgeführt sind. Wenn Sie für ein Unterverzeichnis Sicherheitseinstellungen anpassen möchten, die sich von den Sicherheitseinstellungen des übergeordneten Verzeichnisses unterscheiden, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Durch Klicken auf die Schaltfläche **Löschen** wird der ausgewählte Bereich von Untersuchungen 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.

Parameter	Description
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 Anwendung. Wenn das Kontrollkästchen aktiviert ist, verarbeitet die Anwendung diesen Untersuchungsbereich während ihrer Ausführung. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die Anwendung 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. Dieses 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. Standardmäßige Pfadangabe **/** – Die Anwendung 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 Anwendung 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 Anwendung während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske ***** (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

So verwenden Sie Tags

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Wobei gilt:

`<id>` ist die Container-ID.

`<name>` ist ein Containername

`<path to local directory>` ist der Pfad zum lokalen Verzeichnis.

Sie können auch eindeutige Kombinationen von Tags verwenden: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` und `[image-name:<name>]/path to local directory>`.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispielsweise:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

Fenster "Untersuchungseinstellungen"

In diesem Fenster können Sie die Einstellungen für die Untersuchung von Dateien durch den Schutz vor bedrohlichen Dateien konfigurieren.

Parameter	Description
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 Anwendung entpackt werden, was die Untersuchung verlangsamen kann. Sie können die Dauer der Untersuchung von Archiven reduzieren, indem Sie im Block **Allgemeine Untersuchungseinstellungen** die Einstellungen **Datei überspringen, wenn Untersuchung länger dauert als (Sek.)** und/oder **Datei überspringen, wenn diese größer ist als (MB)** aktivieren und konfigurieren. Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security Archive nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Selbstentpackende Archive (SFX) 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 mit 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 Programmprotokollen optimieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security Textdateien. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Dieser Parameter wird angewendet, wenn Sie den Mechanismus zum Abfangen von Systemereignissen auf Basis der fanotify-Technologie verwenden. Bei Verwendung des aktualisierbaren Kernel-Moduls wird die Untersuchung durch die Zwischenspeicherung von Untersuchungsergebnissen optimiert.
Protokolldateien von Datenbanken überspringen	Schließt Protokolldateien von Datenbanken vorübergehend von der Untersuchung aus. Wenn das Kontrollkästchen aktiviert ist, untersucht die Anwendung keine Datenbankprotokolldateien, wenn diese Protokolldateien innerhalb von 10 Minuten nach der letzten Untersuchung von demselben Prozess erneut verwendet werden. Mit diesem Parameter können Sie die Untersuchung von Datenbankprotokollen optimieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung die Datenbankprotokolldateien. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Dieser Parameter wird angewendet, wenn Sie den Mechanismus zum Abfangen von Systemereignissen auf Basis der fanotify-Technologie verwenden. Bei Verwendung des aktualisierbaren Kernel-Moduls wird die Untersuchung durch die Zwischenspeicherung von Untersuchungsergebnissen optimiert.
Datei überspringen, wenn 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.

Parameter	Description
Datei überspringen, wenn diese größer ist 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 oder 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 oder 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 oder 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. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Heuristische Analyse verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die heuristische Analyse bei der Untersuchung von Dateien. Dieses 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 gewährleistet eine optimale Kombination aus Schutzqualität und Auswirkung auf die Leistung der geschützten Geräte.

Fenster "Aktionen beim Erkennen von Bedrohungen"

In diesem Fenster können Sie Aktionen auswählen, die von der Anwendung Kaspersky Endpoint Security für gefundene infizierte Objekte ausgeführt werden soll.

Einstellungen für den Schutz vor bedrohlichen Dateien

Parameter	Description
Aktionen beim Erkennen von Bedrohungen	Sie können Aktionen auswählen, die von der Anwendung auf gefundene infizierte Objekte anwenden soll: • **Desinfizieren. Entfernen, wenn Desinfektion fehlschlägt** (Standardwert). Wenn Sie diese Aktion auswählen, versucht die Anwendung, das infizierte Objekt zu desinfizieren, indem sie eine Kopie des Objekts im Backup-Speicher speichert. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), löscht die Anwendung das Objekt. • **Desinfizieren. Blockieren, wenn Desinfektion fehlschlägt**. Wenn Sie diese Aktion auswählen, versucht die Anwendung, das infizierte Objekt zu desinfizieren, indem sie eine Kopie des Objekts im Backup-Speicher speichert. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), blockiert die Anwendung den Zugriff auf das Objekt. • **Blockieren**. Wenn Sie diese Aktion auswählen, blockiert die Anwendung den Zugriff auf das infizierte Objekt. Bei einer Desinfektion und Löschung wird eine Kopie des infizierten Objekts im Backup-Speicher gespeichert.

Ausschlüsse aus dem Schutz vor bedrohlichen Dateien

Ein *Ausschluss aus dem Schutz* ist eine Reihe von Bedingungen, die erfüllt sein müssen, damit die Anwendung 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 Ausnahmen für den Schutz vor bedrohlichen Dateien in den Eigenschaften der Richtlinie konfigurieren (**Basisschutz → Ausnahmen des Schutzes vor bedrohlichen Dateien**).

Einstellungen der Ausnahmen von der Untersuchung

Einstellungsgruppe	Description
Ausnahmen	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster Ausnahmebereiche geöffnet. In diesem Fenster können Sie eine Liste mit Bereichen festlegen, die von der Untersuchung ausgeschlossen werden sollen.
Ausnahmen 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.
Ausnahmen nach Name der Bedrohung	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 Ausnahmen nach Prozess öffnet. In diesem Fenster können Sie den Ausschluss der Aktivität von Prozessen aus der Untersuchung konfigurieren.

Fenster "Ausschlussbereiche"

Das Fenster enthält die Ausschlussbereiche einer Untersuchung. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden.

Einstellungen des Ausschlussbereichs

Parameter	Description
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Path	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der Anwendung angewendet wird.

Standardmäßig ist die Tabelle mit den Ausschlussbereichen leer. Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

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 „Neuer Ausnahmebereich“

In diesem Fenster können Sie einen neuen Bereich mit Untersuchungsausschlüssen hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs

Parameter	Description
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 Anwendung. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während ihrer Ausführung von der Untersuchung aus. Wenn das Kontrollkästchen deaktiviert ist, schließt die Anwendung diesen Bereich während ihrer Ausführung in die Untersuchung ein. Sie können diesen Bereich zu einem späteren Zeitpunkt ausschließen, indem Sie das Kontrollkästchen aktivieren. Dieses 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. 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 Anwendung 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.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

So verwenden Sie Tags

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Wobei gilt:

`<id>` ist die Container-ID.

`<name>` ist ein Containername

`<path to local directory>` ist der Pfad zum lokalen Verzeichnis.

Sie können auch eindeutige Kombinationen von Tags verwenden: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` und `[image-name:<name>]/path to local directory>`.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispielsweise:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

Fenster "Ausnahmen nach Maske"

Sie können eine Namensmaske verwenden, um Untersuchungsausnahmen für Objekte zu 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 **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).

Sie können die Vereinigung der Ausschlusslisten aktivieren, wenn diese von untergeordneten Richtlinien geerbt werden. Um die Listenelemente zu vereinigen, muss das Kontrollkästchen **Werte beim Vererben vereinigen aktiviert** sein. Wenn das Kontrollkästchen aktiviert ist, werden die Elemente der übergeordneten Richtlinienliste in den untergeordneten Richtlinien angezeigt und die Elemente können der untergeordneten Richtlinienliste hinzugefügt werden. Bei deaktiviertem Kontrollkästchen werden die Listenelemente beim Vererben von Richtlinieneinstellungen nicht vereinigt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Fenster "Ausschlüsse nach Bedrohungsname"

Sie können den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren. Die Anwendung blockiert die angegebenen Bedrohungen nicht. Standardmäßig ist die Liste mit den Namen von Bedrohungen leer.

Sie können Namen von Bedrohungen hinzufügen, bearbeiten und löschen.

Sie können die Vereinigung der Ausschlusslisten aktivieren, wenn diese von untergeordneten Richtlinien geerbt werden. Um die Listenelemente zu vereinigen, muss das Kontrollkästchen **Werte beim Vererben vereinigen aktiviert** sein. Wenn das Kontrollkästchen aktiviert ist, werden die Elemente der übergeordneten Richtlinienliste in den untergeordneten Richtlinien angezeigt und die Elemente können der untergeordneten Richtlinienliste hinzugefügt werden. Bei deaktiviertem Kontrollkästchen werden die Listenelemente beim Vererben von Richtlinieneinstellungen nicht vereinigt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Fenster "Ausnahmen nach Prozess"

Das Fenster 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 Liste zwei Ausschlussbereiche, welche die Pfade zu Administrationsagenten enthalten. Bei Bedarf können Sie diesen Ausschluss entfernen.

Einstellungen des Ausschlussbereichs nach Prozessen

Parameter	Description
Werte bei Vererbung vereinen	Das Kontrollkästchen aktiviert oder deaktiviert die Vereinigung der Liste, wenn diese von untergeordneten Richtlinien geerbt wird. Wenn das Kontrollkästchen aktiviert ist, werden die Elemente der übergeordneten Richtlinienliste in den untergeordneten Richtlinien angezeigt und die Elemente können der untergeordneten Richtlinienliste hinzugefügt werden. Bei deaktiviertem Kontrollkästchen werden die Listenelemente beim Vererben von Richtlinieneinstellungen nicht vereinigt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Path	Vollständiger Pfad des auszuschließenden Prozesses.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der Anwendung angewendet wird.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

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

Parameter	Description
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle 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. Wenn für das Abfangen von Systemereignissen das aktualisierbare Kernel-Modul verwendet wird, wird der angegebene Prozess in allen Namensräumen vom Abfangen ausgeschlossen.
Auf untergeordnete Prozesse anwenden	Untergeordnete Prozesse des ausgeschlossenen Prozesses, der durch den Parameter **Pfad des auszuschließenden Prozesses** angegeben ist, 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 Anwendung. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während ihrer Ausführung von der Untersuchung aus. Wenn das Kontrollkästchen deaktiviert ist, schließt die Anwendung diesen Bereich während ihrer Ausführung in die Untersuchung ein. Sie können diesen Bereich zu einem späteren Zeitpunkt ausschließen, indem Sie das Kontrollkästchen aktivieren. Dieses 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 Masken verwendet werden. Das Eingabefeld darf nicht leer sein.
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 Anwendung 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.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Schadsoftware-Untersuchung

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 verwalten, indem Sie die Einstellungen der Aufgaben bearbeiten.

In den Eigenschaften der Aufgabe *Nach Malware suchen* können Sie im Abschnitt **Einstellungen** die in der folgenden Tabelle aufgeführten Einstellungen verwalten.

Untersuchungsparameter der Aufgabe zur Schadsoftware-Untersuchung

Parameter	Description
Untersuchung	Diese Einstellungsgruppe enthält Schaltflächen, mit denen Fenster geöffnet werden, in denen Sie die Untersuchungsbereiche, die Einstellungen des Untersuchungsbereichs und die Untersuchungseinstellungen konfigurieren können.
Aktionen beim Erkennen von Bedrohungen	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Aktionen beim Erkennen von Bedrohungen** geöffnet, in dem Sie die Aktionen konfigurieren können, die die App für erkannte infizierte Objekte ausführt.

In den Eigenschaften der Aufgabe *Nach Malware suchen* können Sie im Abschnitt **Ausnahmen** Ausnahmebereiche, Ausnahmen nach Maske und 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

Parameter	Description
Name des Bereichs	Name des Untersuchungsbereichs
Path	Der Pfad zu dem zu untersuchenden Verzeichnis.
Status	Der Status gibt an, ob die Anwendung 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 aufgeführt sind. Wenn Sie für ein Unterverzeichnis Sicherheitseinstellungen anpassen möchten, die sich von den Sicherheitseinstellungen des übergeordneten Verzeichnisses unterscheiden, 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 aufgeführt sind. Wenn Sie für ein Unterverzeichnis Sicherheitseinstellungen anpassen möchten, die sich von den Sicherheitseinstellungen des übergeordneten Verzeichnisses unterscheiden, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Durch Klicken auf die Schaltfläche **Löschen** wird der ausgewählte Bereich von Untersuchungen 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

Parameter	Description
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 Anwendung. Wenn das Kontrollkästchen aktiviert ist, verarbeitet die Anwendung diesen Untersuchungsbereich während ihrer Ausführung. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die Anwendung 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. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Parameter	Description
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. Standardmäßige Pfadangabe **/** – Die Anwendung 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 Anwendung 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 Anwendung während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

So verwenden Sie Tags

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Wobei gilt:

`<id>` ist die Container-ID.

`<name>` ist ein Containername

`<path to local directory>` ist der Pfad zum lokalen Verzeichnis.

Sie können auch eindeutige Kombinationen von Tags verwenden: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` und `[image-name:<name>]/path to local directory>`.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispielsweise:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

Fenster "Einstellungen des Untersuchungsbereichs"

In diesem Fenster können Sie die Einstellungen für die Untersuchung während der Ausführung der Aufgabe zur Schadsoftware-Untersuchung konfigurieren. Die Anwendung ermöglicht die Untersuchung von Dateien, Bootsektoren, Gerätespeicher und Autostart-Objekten.

Einstellungen des Untersuchungsbereichs

Parameter	Description
Dateien untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Dateien. Wenn das Kontrollkästchen aktiviert ist, untersucht das Programm Dateien. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Dateien. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Parameter	Description
Bootsektoren untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Bootsektoren. Wenn das Kontrollkästchen aktiviert ist, untersucht das Programm die Bootsektoren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Bootsektoren. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Kernel-Speicher und gestartete Prozesse untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung des Arbeitsspeichers des Geräts. Wenn diese Option aktiviert ist, überprüft die Anwendung 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 das Programm Autostart-Objekte. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Autostart-Objekte. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Zu untersuchende Geräte	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Untersuchungsbereiche** geöffnet, in dem Sie die Geräte angeben können, deren Bootsektoren untersucht werden müssen.
Globale Ausnahmen verwenden	Das Kontrollkästchen aktiviert oder deaktiviert den Ausschluss von in den globalen Ausnahmen angegeben Mountpunkten während der Anwendungsausführung. Wenn diese Option aktiviert ist, schließt die Anwendung die konfigurierten Mountpunkte von der Untersuchung aus. Dieses 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 Anwendungsausführung. Wenn das Kontrollkästchen aktiviert ist, schließt die Anwendung jene Objekte von der Untersuchung aus, die in den Ausschlüssen der Komponente "Schutz vor bedrohlichen Dateien" angegeben sind. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält die Masken der Gerätenamen, deren Bootsektoren die Anwendung untersuchen soll. Standardmäßig enthält die Tabelle die Gerätenamen-Maske **/**** (alle Geräte).

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Fenster "Untersuchungseinstellungen"

In diesem Fenster können Sie die Einstellungen für die Untersuchung von Dateien durch die Aufgabe konfigurieren.

Untersuchungseinstellungen

Parameter	Description
Archive untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Archiven. Wenn das Kontrollkästchen aktiviert ist, so untersucht die Anwendung Archive. Um ein Archiv zu untersuchen, muss es zunächst von der Anwendung entpackt werden, was die Untersuchung verlangsamen kann. Sie können die Dauer der Untersuchung von Archiven verkürzen, indem Sie die Einstellungen **Datei überspringen, wenn Untersuchung länger dauert als (Sek.)** und **Datei überspringen, wenn diese größer ist als (MB)** im Abschnitt **Allgemeine Untersuchungseinstellungen** konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Archive. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Parameter	Description
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 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 Anwendung 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 Anwendung E-Mail-Nachrichten im Textformat nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Datei überspringen, wenn 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 Anwendung die Untersuchung der Datei ab. Zulässige Werte: 0 – 9999. Ist der Wert 0 angegeben, dann ist die Untersuchungsdauer nicht beschränkt. Standardwert: 0.
Datei überspringen, wenn diese größer ist 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 Anwendung Dateien jeder Größe. Standardwert: 0.
Virenfreie Objekte protokollieren	Dieses Kontrollkästchen aktiviert oder deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectProcessed*. Wenn das Kontrollkästchen aktiviert ist, protokolliert die Anwendung Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die Anwendung keine Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Unverarbeitete Objekte protokollieren	Dieses Kontrollkästchen aktiviert oder 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 Anwendung Ereignisse vom Typ *ObjectNotProcessed*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die Anwendung keine Ereignisse vom Typ *ObjectNotProcessed*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Gepackte Objekte protokollieren	Dieses Kontrollkästchen aktiviert oder deaktiviert die Protokollierung der Ereignisse vom Typ *PackedObjectDetected* für alle erkannten gepackten Objekte. Wenn das Kontrollkästchen aktiviert ist, protokolliert die Anwendung Ereignisse vom Typ *PackedObjectDetected*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die Anwendung 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 das Programm nur neue Dateien oder Dateien, die seit der letzten Untersuchung geändert wurden. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung Dateien unabhängig von ihrem Erstellungs- oder Änderungsdatum. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Heuristische Analyse verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die heuristische Analyse bei der Untersuchung von Dateien. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Parameter	Description
Stufe der heuristischen Analyse	Wenn das Kontrollkästchen **Heuristische Analyse verwenden** aktiviert ist, können Sie in der Dropdown-Liste die Stufe der heuristischen Analyse auswählen: • **Oberflächlich** ist die am wenigsten genaue Untersuchung mit minimaler Systembelastung. • **Mittel** ist eine mittlere Untersuchung mit ausgewogener Systembelastung. • **Tief** ist die genaueste Untersuchung mit maximaler Systembelastung. • **Empfohlen** (Standardwert) ist die optimale Stufe, die von Kaspersky-Experten empfohlen wird. Sie gewährleistet eine optimale Kombination aus Schutzqualität und Auswirkung auf die Leistung der geschützten Geräte.
Nicht mehrere Untersuchungsaufgaben gleichzeitig ausführen	Aufgeschobener Start von Untersuchungsaufgaben, wenn bereits eine Untersuchungsaufgabe ausgeführt wird. Kaspersky Endpoint Security reiht neue Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Beispiel: Das Programm hat nach Zeitplan eine vollständige Untersuchungsaufgabe gestartet. Wenn ein Benutzer versucht, eine schnelle Untersuchung über die Programmoberfläche zu starten, stellt Kaspersky Endpoint Security diese Aufgabe zur schnellen Untersuchung in die Warteschlange und startet diese Aufgabe automatisch, nachdem die vollständige Untersuchungsaufgabe abgeschlossen wurde. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Fenster "Aktionen beim Erkennen von Bedrohungen"

In diesem Fenster können Sie Aktionen auswählen, die von der Anwendung Kaspersky Endpoint Security für gefundene infizierte Objekte ausgeführt werden soll.

Aktionen beim Erkennen von Bedrohungen

Parameter	Description
Aktionen beim Erkennen von Bedrohungen	Sie können Aktionen auswählen, die von der Anwendung auf gefundene infizierte Objekte anwenden soll: • **Desinfizieren. Entfernen, wenn Desinfektion fehlschlägt** (Standardwert). Wenn Sie diese Aktion auswählen, versucht die Anwendung, das infizierte Objekt zu desinfizieren, indem sie eine Kopie des Objekts im Backup-Speicher speichert. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), löscht die Anwendung das Objekt. • **Desinfizieren. Informieren, wenn Desinfektion fehlschlägt**. Wenn Sie diese Aktion auswählen, versucht die Anwendung, das infizierte Objekt zu desinfizieren, indem sie eine Kopie des Objekts im Backup-Speicher speichert. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), speichert die Anwendung Informationen darüber im Protokoll. • **Informieren**. Wenn Sie diese Aktion auswählen, speichert die Anwendung Informationen über das infizierte Objekt im Protokoll.

Abschnitt "Ausnahmen"

Eine *Untersuchungsausnahme* ist eine Reihe von Bedingungen. Wenn diese Bedingungen erfüllt sind, untersucht Kaspersky Endpoint Security die Objekte nicht auf Viren und andere Malware. Objekte können auch anhand von Masken und Bedrohungsnamen von der Untersuchung ausgeschlossen werden.

Einstellungen der Ausnahmen von der Untersuchung

Einstellungsgruppe	Description
Ausschlussbereiche	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Ausnahmebereiche** geöffnet. In diesem Fenster können Sie eine Liste mit Bereichen festlegen, die von der Untersuchung ausgeschlossen werden sollen.
Ausnahmen 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.
Ausnahmen nach Name der Bedrohung	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"

Das Fenster enthält die Ausschlussbereiche einer Untersuchung. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden.

Einstellungen des Ausschlussbereichs

Parameter	Description
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Path	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der Anwendung angewendet wird.

Standardmäßig ist die Tabelle mit den Ausschlussbereichen leer. Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

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 „Neuer Ausnahmebereich“

In diesem Fenster können Sie einen neuen Bereich mit Untersuchungsausschlüssen hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs

Parameter	Description
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 Anwendung. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während ihrer Ausführung von der Untersuchung aus. Wenn das Kontrollkästchen deaktiviert ist, schließt die Anwendung diesen Bereich während ihrer Ausführung in die Untersuchung ein. Sie können diesen Bereich zu einem späteren Zeitpunkt ausschließen, indem Sie das Kontrollkästchen aktivieren. Dieses 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. Als Pfad ist standardmäßig **/** angegeben. Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus.

Parameter	Description
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 Anwendung 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.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

So verwenden Sie Tags

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Wobei gilt:

`<id>` ist die Container-ID.

`<name>` ist ein Containername

`<path to local directory>` ist der Pfad zum lokalen Verzeichnis.

Sie können auch eindeutige Kombinationen von Tags verwenden: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` und `[image-name:<name>]/path to local directory>`.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispielsweise:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

Fenster "Ausnahmen nach Maske"

Sie können eine Namensmaske verwenden, um Untersuchungsausnahmen für Objekte zu konfigurieren. Die Anwendung 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 **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 Anwendung blockiert die angegebenen Bedrohungen nicht. Standardmäßig ist die Liste mit den Namen von Bedrohungen leer.

Sie können Namen von Bedrohungen hinzufügen, bearbeiten und löschen.

Untersuchung wichtiger Bereiche

In der Verwaltungskonsole können Sie mithilfe der Aufgabe *Untersuchung wichtiger Bereiche* wichtige Bereiche des Betriebssystems des geschützten Geräts untersuchen.

Sie können benutzerdefinierte Aufgaben zur Untersuchung wichtiger Bereiche erstellen und ausführen. Sie können die Untersuchungseinstellungen verwalten, indem Sie die Einstellungen der Aufgaben bearbeiten.

In den Eigenschaften der Aufgabe *Untersuchung wichtiger Bereiche* können Sie im Abschnitt **Einstellungen** die in der folgenden Tabelle aufgeführten Einstellungen verwalten.

Einstellungen der Aufgabe zur Untersuchung wichtiger Bereiche

Parameter	Description
Untersuchung	Diese Einstellungsgruppe enthält Schaltflächen, mit denen Fenster geöffnet werden, in denen Sie die Untersuchungsbereiche, die Einstellungen des Untersuchungsbereichs und die Untersuchungseinstellungen konfigurieren können.
Aktionen beim Erkennen von Bedrohungen	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Aktionen beim Erkennen von Bedrohungen** geöffnet, in dem Sie die Aktionen konfigurieren können, die die App für erkannte infizierte Objekte ausführt.

In den Eigenschaften der Aufgabe *Untersuchung wichtiger Bereiche* können Sie im Abschnitt **Ausnahmen** Ausschlussbereiche, Ausnahmen nach Maske und 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

Parameter	Description
Name des Bereichs	Name des Untersuchungsbereichs
Path	Der Pfad zu dem zu untersuchenden Verzeichnis.
Status	Der Status gibt an, ob die Anwendung 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 aufgeführt sind. Wenn Sie für ein Unterverzeichnis Sicherheitseinstellungen anpassen möchten, die sich von den Sicherheitseinstellungen des übergeordneten Verzeichnisses unterscheiden, 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 aufgeführt sind. Wenn Sie für ein Unterverzeichnis Sicherheitseinstellungen anpassen möchten, die sich von den Sicherheitseinstellungen des übergeordneten Verzeichnisses unterscheiden, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Durch Klicken auf die Schaltfläche **Löschen** wird der ausgewählte Bereich von Untersuchungen 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

Parameter	Description
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 Anwendung. Wenn das Kontrollkästchen aktiviert ist, verarbeitet die Anwendung diesen Untersuchungsbereich während ihrer Ausführung. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die Anwendung 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. Dieses 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. Standardmäßige Pfadangabe **/** – Die Anwendung 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 Anwendung 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 Anwendung während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

So verwenden Sie Tags

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Wobei gilt:

`<id>` ist die Container-ID.

`<name>` ist ein Containername

`<path to local directory>` ist der Pfad zum lokalen Verzeichnis.

Sie können auch eindeutige Kombinationen von Tags verwenden: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` und `[image-name:<name>]/path to local directory>`.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispielsweise:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

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 Anwendung ermöglicht die Untersuchung der Dateien, Bootsektoren, der Autostart-Objekte, des Prozess- und des Kernelspeichers.

Einstellungen des Untersuchungsbereichs

Parameter	Description
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. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Kernel-Speicher 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. Dieses 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. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Zu untersuchende Geräte	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Untersuchungsbereiche** geöffnet, in dem Sie die Geräte angeben können, deren Bootsektoren untersucht werden müssen.
Globale Ausnahmen verwenden	Das Kontrollkästchen aktiviert oder deaktiviert den Ausschluss von in den globalen Ausnahmen angegeben Mountpunkten während der Anwendungsausführung. Wenn diese Option aktiviert ist, schließt die Anwendung die konfigurierten Mountpunkte von der Untersuchung aus. Dieses 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 Anwendungsausführung. Wenn das Kontrollkästchen aktiviert ist, schließt die Anwendung jene Objekte von der Untersuchung aus, die in den Ausschlüssen der Komponente "Schutz vor bedrohlichen Dateien" angegeben sind. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält die Masken der Gerätenamen, deren Bootsektoren die Anwendung untersuchen soll. Standardmäßig enthält die Tabelle die Gerätenamen-Maske **/**** (alle Geräte).

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Fenster "Untersuchungseinstellungen"

In diesem Fenster können Sie die Einstellungen für die Untersuchung von Dateien durch die Aufgabe konfigurieren.

Parameter	Description
Archive untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Archiven. Wenn das Kontrollkästchen aktiviert ist, so untersucht die Anwendung Archive. Um ein Archiv zu untersuchen, muss es zunächst von der Anwendung entpackt werden, was die Untersuchung verlangsamen kann. Sie können die Dauer der Untersuchung von Archiven verkürzen, indem Sie die Einstellungen **Datei überspringen, wenn Untersuchung länger dauert als (Sek.)** und **Datei überspringen, wenn diese größer ist als (MB)** im Abschnitt **Allgemeine Untersuchungseinstellungen** konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Archive. Dieses 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. Dieses 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 Anwendung 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 Anwendung E-Mail-Nachrichten im Textformat nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Datei überspringen, wenn 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 Anwendung die Untersuchung der Datei ab. Zulässige Werte: 0 – 9999. Ist der Wert 0 angegeben, dann ist die Untersuchungsdauer nicht beschränkt. Standardwert: 0.
Datei überspringen, wenn diese größer ist 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 Anwendung Dateien jeder Größe. Standardwert: 0.
Virenfreie Objekte protokollieren	Dieses Kontrollkästchen aktiviert oder deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectProcessed*. Wenn das Kontrollkästchen aktiviert ist, protokolliert die Anwendung Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die Anwendung keine Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Unverarbeitete Objekte protokollieren	Dieses Kontrollkästchen aktiviert oder 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 Anwendung Ereignisse vom Typ *ObjectNotProcessed*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die Anwendung keine Ereignisse vom Typ *ObjectNotProcessed*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Gepackte Objekte protokollieren	Dieses Kontrollkästchen aktiviert oder deaktiviert die Protokollierung der Ereignisse vom Typ *PackedObjectDetected* für alle erkannten gepackten Objekte. Wenn das Kontrollkästchen aktiviert ist, protokolliert die Anwendung Ereignisse vom Typ *PackedObjectDetected*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die Anwendung keine Ereignisse vom Typ *PackedObjectDetected*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Parameter	Description
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 das Programm nur neue Dateien oder Dateien, die seit der letzten Untersuchung geändert wurden. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung Dateien unabhängig von ihrem Erstellungs- oder Änderungsdatum. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Heuristische Analyse verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die heuristische Analyse bei der Untersuchung von Dateien. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Stufe der heuristischen Analyse	Wenn das Kontrollkästchen **Heuristische Analyse verwenden** aktiviert ist, können Sie in der Dropdown-Liste die Stufe der heuristischen Analyse auswählen: • **Oberflächlich** ist die am wenigsten genaue Untersuchung mit minimaler Systembelastung. • **Mittel** ist eine mittlere Untersuchung mit ausgewogener Systembelastung. • **Tief** ist die genaueste Untersuchung mit maximaler Systembelastung. • **Empfohlen** (Standardwert) ist die optimale Stufe, die von Kaspersky-Experten empfohlen wird. Sie gewährleistet eine optimale Kombination aus Schutzqualität und Auswirkung auf die Leistung der geschützten Geräte.
Nicht mehrere Untersuchungsaufgaben gleichzeitig ausführen	Aufgeschobener Start von Untersuchungsaufgaben, wenn bereits eine Untersuchungsaufgabe ausgeführt wird. Kaspersky Endpoint Security reiht neue Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Beispiel: Das Programm hat nach Zeitplan eine vollständige Untersuchungsaufgabe gestartet. Wenn ein Benutzer versucht, eine schnelle Untersuchung über die Programmoberfläche zu starten, stellt Kaspersky Endpoint Security diese Aufgabe zur schnellen Untersuchung in die Warteschlange und startet diese Aufgabe automatisch, nachdem die vollständige Untersuchungsaufgabe abgeschlossen wurde. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Fenster "Aktionen beim Erkennen von Bedrohungen"

In diesem Fenster können Sie Aktionen auswählen, die von der Anwendung Kaspersky Endpoint Security für gefundene infizierte Objekte ausgeführt werden soll.

Aktionen beim Erkennen von Bedrohungen

Parameter	Description
Aktionen beim Erkennen von Bedrohungen	Sie können Aktionen auswählen, die von der Anwendung auf gefundene infizierte Objekte anwenden soll: • **Desinfizieren. Entfernen, wenn Desinfektion fehlschlägt** (Standardwert). Wenn Sie diese Aktion auswählen, versucht die Anwendung, das infizierte Objekt zu desinfizieren, indem sie eine Kopie des Objekts im Backup-Speicher speichert. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), löscht die Anwendung das Objekt. • **Desinfizieren. Informieren, wenn Desinfektion fehlschlägt**. Wenn Sie diese Aktion auswählen, versucht die Anwendung, das infizierte Objekt zu desinfizieren, indem sie eine Kopie des Objekts im Backup-Speicher speichert. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), speichert die Anwendung Informationen darüber im Protokoll. • **Informieren**. Wenn Sie diese Aktion auswählen, speichert die Anwendung Informationen über das infizierte Objekt im Protokoll.

Abschnitt "Ausnahmen"

Eine *Untersuchungsausnahme* ist eine Reihe von Bedingungen. Wenn diese Bedingungen erfüllt sind, untersucht Kaspersky Endpoint Security die Objekte nicht auf Viren und andere Malware. Objekte können auch anhand von Masken und Bedrohungsnamen von der Untersuchung ausgeschlossen werden.

Einstellungen der Ausnahmen von der Untersuchung

Einstellungsgruppe	Description
Ausschlussbereiche	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster Ausnahmebereiche geöffnet. In diesem Fenster können Sie eine Liste mit Bereichen festlegen, die von der Untersuchung ausgeschlossen werden sollen.
Ausnahmen 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.
Ausnahmen nach Name der Bedrohung	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"

Das Fenster enthält die Ausschlussbereiche einer Untersuchung. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden.

Einstellungen des Ausschlussbereichs

Parameter	Description
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Path	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der Anwendung angewendet wird.

Standardmäßig ist die Tabelle mit den Ausschlussbereichen leer. Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

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 „Neuer Ausnahmebereich“

In diesem Fenster können Sie einen neuen Bereich mit Untersuchungsausschlüssen hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs

Parameter	Description
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 Anwendung. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während ihrer Ausführung von der Untersuchung aus. Wenn das Kontrollkästchen deaktiviert ist, schließt die Anwendung diesen Bereich während ihrer Ausführung in die Untersuchung ein. Sie können diesen Bereich zu einem späteren Zeitpunkt ausschließen, indem Sie das Kontrollkästchen aktivieren. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Parameter	Description
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. 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 Anwendung 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.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

So verwenden Sie Tags

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Wobei gilt:

`<id>` ist die Container-ID.

`<name>` ist ein Containername

`<path to local directory>` ist der Pfad zum lokalen Verzeichnis.

Sie können auch eindeutige Kombinationen von Tags verwenden: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` und `[image-name:<name>]/path to local directory>`.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispielsweise:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

Fenster "Ausnahmen nach Maske"

Sie können eine Namensmaske verwenden, um Untersuchungsausnahmen für Objekte zu konfigurieren. Die Anwendung 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 **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 Anwendung blockiert die angegebenen Bedrohungen nicht. Standardmäßig ist die Liste mit den Namen von Bedrohungen leer.

Sie können Namen von Bedrohungen hinzufügen, bearbeiten und löschen.

Container-Überwachung

In der Verwaltungskonsole können Sie die Komponente „Container-Überwachung“ in den Eigenschaften der Richtlinie konfigurieren (**Allgemeine Einstellungen → Einstellungen der Untersuchung von Containern**).

Einstellungen der Container-Überwachung

Parameter	Description
Untersuchung von Namensräumen und Containern aktivieren	Dieses Kontrollkästchen aktiviert oder deaktiviert die Untersuchung von Namespaces und Containern in Echtzeit. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Aktion für einen Container bei 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 Anwendung den Container an. • **Container anhalten, falls Desinfektion fehlschlägt** (Standardwert) – Wenn die Desinfektion eines infizierten Objekts fehlgeschlagen ist, hält die Anwendung den Container an. Dieser Parameter ist verfügbar, wenn die Anwendung im Rahmen einer Lizenz verwendet wird, von der diese Funktion abgedeckt wird.
Einstellungen der Untersuchung von Containern	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Einstellungen der Untersuchung von Containern** geöffnet.

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

Parameter	Description
Docker verwenden	Dieses Kontrollkästchen aktiviert oder deaktiviert die Verwendung des Systems zur Verwaltung von Docker-Containern. Dieses 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. Dieses 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. Dieses 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. Standardwert: /var/lib/containers/storage

Parameter	Description
Runc verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Verwendung des runc-Tools. Dieses 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 untersuchen

In der Verwaltungskonsole können Sie Container und Images mithilfe der Aufgabe *Untersuchung von Containern* untersuchen.

Sie können benutzerdefinierte Aufgaben zur Untersuchung von Containern erstellen und ausführen. Sie können die Untersuchungseinstellungen verwalten, indem Sie die Einstellungen der Aufgaben bearbeiten.

In den Eigenschaften der Aufgabe *Untersuchung von Containern* können Sie im Abschnitt **Einstellungen** die in der folgenden Tabelle aufgeführten Einstellungen verwalten.

Einstellungen der Aufgabe zur Untersuchung von Containern

Parameter	Description
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.
Aktionen beim Erkennen von Bedrohungen	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Aktionen beim Erkennen von Bedrohungen** geöffnet, in dem Sie die Aktionen konfigurieren können, die die App für erkannte infizierte Objekte ausführt.

In den Eigenschaften der Aufgabe *Untersuchung von Containern* können Sie im Abschnitt **Ausnahmen** außerdem Ausnahmen 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

Parameter	Description
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. Dieses 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).

Parameter	Description
Aktion 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** – keine Aktionen 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 empfohlen, 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. Dieses 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 Fund einer Bedrohung	In dieser Dropdown-Liste können Sie eine Aktion auswählen, die von der Anwendung 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.
Jeden Layer 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

Parameter	Description
Archive untersuchen	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung von Archiven. Wenn das Kontrollkästchen aktiviert ist, so untersucht die Anwendung Archive. Um ein Archiv zu untersuchen, muss es zunächst von der Anwendung entpackt werden, was die Untersuchung verlangsamen kann. Sie können die Dauer der Untersuchung von Archiven verkürzen, indem Sie die Einstellungen **Datei überspringen, wenn Untersuchung länger dauert als (Sek.)** und **Datei überspringen, wenn diese größer ist als (MB)** im Abschnitt **Allgemeine Untersuchungseinstellungen** konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Archive. Dieses 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. Dieses 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 Anwendung keine Dateien von Mail-Datenbanken. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Parameter	Description
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 Anwendung E-Mail-Nachrichten im Textformat nicht. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Datei überspringen, wenn 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 Anwendung die Untersuchung der Datei ab. Zulässige Werte: 0 – 9999. Ist der Wert 0 angegeben, dann ist die Untersuchungsdauer nicht beschränkt. Standardwert: 0.
Datei überspringen, wenn diese größer ist 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 Anwendung Dateien jeder Größe. Standardwert: 0.
Virenfreie Objekte protokollieren	Dieses Kontrollkästchen aktiviert oder deaktiviert die Protokollierung der Ereignisse vom Typ *ObjectProcessed*. Wenn das Kontrollkästchen aktiviert ist, protokolliert die Anwendung Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die Anwendung keine Ereignisse vom Typ *ObjectProcessed* für jedes untersuchte Objekt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Unverarbeitete Objekte protokollieren	Dieses Kontrollkästchen aktiviert oder 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 Anwendung Ereignisse vom Typ *ObjectNotProcessed*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die Anwendung keine Ereignisse vom Typ *ObjectNotProcessed*. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Gepackte Objekte protokollieren	Dieses Kontrollkästchen aktiviert oder deaktiviert die Protokollierung der Ereignisse vom Typ *PackedObjectDetected* für alle erkannten gepackten Objekte. Wenn das Kontrollkästchen aktiviert ist, protokolliert die Anwendung Ereignisse vom Typ *PackedObjectDetected*. Wenn das Kontrollkästchen deaktiviert ist, protokolliert die Anwendung 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 das Programm nur neue Dateien oder Dateien, die seit der letzten Untersuchung geändert wurden. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung Dateien unabhängig von ihrem Erstellungs- oder Änderungsdatum. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Heuristische Analyse verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die heuristische Analyse bei der Untersuchung von Dateien. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Stufe der heuristischen Analyse	Wenn das Kontrollkästchen **Heuristische Analyse verwenden** aktiviert ist, können Sie in der Dropdown-Liste die Stufe der heuristischen Analyse auswählen: • **Oberflächlich** ist die am wenigsten genaue Untersuchung mit minimaler Systembelastung. • **Mittel** ist eine mittlere Untersuchung mit ausgewogener Systembelastung. • **Tief** ist die genaueste Untersuchung mit maximaler Systembelastung. • **Empfohlen** (Standardwert) ist die optimale Stufe, die von Kaspersky-Experten empfohlen wird. Sie gewährleistet eine optimale Kombination aus Schutzqualität und Auswirkung auf die Leistung der geschützten Geräte.
Nicht mehrere Untersuchungsaufgaben gleichzeitig ausführen	Aufgeschobener Start von Untersuchungsaufgaben, wenn bereits eine Untersuchungsaufgabe ausgeführt wird. Kaspersky Endpoint Security reiht neue Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Beispiel: Das Programm hat nach Zeitplan eine vollständige Untersuchungsaufgabe gestartet. Wenn ein Benutzer versucht, eine schnelle Untersuchung über die Programmoberfläche zu starten, stellt Kaspersky Endpoint Security diese Aufgabe zur schnellen Untersuchung in die Warteschlange und startet diese Aufgabe automatisch, nachdem die vollständige Untersuchungsaufgabe abgeschlossen wurde. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Fenster "Aktionen beim Erkennen von Bedrohungen"

In diesem Fenster können Sie Aktionen auswählen, die von der Anwendung Kaspersky Endpoint Security für gefundene infizierte Objekte ausgeführt werden soll.

Aktionen beim Erkennen von Bedrohungen

Parameter	Description
Aktionen beim Erkennen von Bedrohungen	Sie können Aktionen auswählen, die von der Anwendung auf gefundene infizierte Objekte anwenden soll: • **Desinfizieren. Entfernen, wenn Desinfektion fehlschlägt** (Standardwert). Wenn Sie diese Aktion auswählen, versucht die Anwendung, das infizierte Objekt zu desinfizieren, indem sie eine Kopie des Objekts im Backup-Speicher speichert. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), löscht die Anwendung das Objekt. • **Desinfizieren. Informieren, wenn Desinfektion fehlschlägt**. Wenn Sie diese Aktion auswählen, versucht die Anwendung, das infizierte Objekt zu desinfizieren, indem sie eine Kopie des Objekts im Backup-Speicher speichert. Wenn die Desinfektion fehlschlägt (beispielsweise, weil der Typ des Objekts oder die Bedrohung im Objekt nicht desinfiziert werden kann), speichert die Anwendung Informationen darüber im Protokoll. • **Informieren**. Wenn Sie diese Aktion auswählen, speichert die Anwendung Informationen über das infizierte Objekt im Protokoll.

Abschnitt "Ausnahmen"

Einstellungen der Ausnahmen von der Untersuchung

Einstellungsgruppe	Description
Ausnahmen 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.
Ausnahmen nach Name der Bedrohung	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 Anwendungsausführung. Wenn diese Option aktiviert ist, schließt die Anwendung die konfigurierten Mountpunkte von der Untersuchung aus. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Fenster "Ausnahmen nach Maske"

Sie können eine Namensmaske verwenden, um Untersuchungsausnahmen für Objekte zu konfigurieren. Die Anwendung 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 **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 Anwendung blockiert die angegebenen Bedrohungen nicht. Standardmäßig ist die Liste mit den Namen von Bedrohungen leer.

Sie können Namen von Bedrohungen hinzufügen, bearbeiten und löschen.

Untersuchung von Wechseldatenträgern

In der Verwaltungskonsole können Sie die Einstellungen für die Untersuchung von Wechseldatenträgern in den Richtlinieneigenschaften konfigurieren (**Lokale Aufgaben → Untersuchung von Wechseldatenträgern**).

Einstellungen der Komponente "Untersuchung von Wechseldatenträgern"

Parameter	Description
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 Verbinden eines Wechseldatenträgers	In der Dropdown-Liste können Sie die Aktion auswählen, die von der Anwendung 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. • **Genaue Untersuchung**: Es werden alle Dateien auf Wechseldatenträgern (außer CD-/DVD-Laufwerken und Blu-ray-Discs) untersucht. 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 Anwendung 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. • **Genaue 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.

Nützliche Artikel

Dateitypen für schnelle Untersuchung

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, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx.

Verhaltensanalyse

In der Verwaltungskonsole können Sie die Einstellungen für die Verhaltensanalyse in den Richtlinieneigenschaften verwalten (**Erweiterter Schutz** → **Verhaltensanalyse**).

Einstellungen der Komponente „Verhaltensanalyse"

Parameter	Description
Verhaltensanalyse aktivieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Komponente "Verhaltensanalyse". Dieses Kontrollkästchen ist standardmäßig aktiviert.
Aktion beim Erkennen eines schädlichen Vorgangs	Aktion, die Kaspersky Endpoint Security ausführen soll, wenn schädliche Aktivitäten im Betriebssystem erkannt werden: • Anwendung, 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.
Ausschlüsse nach Prozessen verwenden	Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung von Ausschlüssen 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 "Ausnahmen nach Prozess"

Das Fenster enthält Ausschlussbereiche nach Prozessen. Mit dem Ausschlussbereich nach Prozessen können Sie einen Untersuchungsausschluss für die Aktivität des angegebenen Prozesses konfigurieren.

Einstellungen des Ausschlussbereichs nach Prozessen

Parameter	Description
Werte bei Vererbung vereinen	Das Kontrollkästchen aktiviert oder deaktiviert die Vereinigung der Liste, wenn diese von untergeordneten Richtlinien geerbt wird. Wenn das Kontrollkästchen aktiviert ist, werden die Elemente der übergeordneten Richtlinienliste in den untergeordneten Richtlinien angezeigt und die Elemente können der untergeordneten Richtlinienliste hinzugefügt werden. Bei deaktiviertem Kontrollkästchen werden die Listenelemente beim Vererben von Richtlinieneinstellungen nicht vereinigt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Path	Vollständiger Pfad des auszuschließenden Prozesses.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der Anwendung angewendet wird.

Standardmäßig ist die Tabelle mit den Ausschlussbereichen leer. Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

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

Parameter	Description
Name des Ausschlussbereichs	Eingabefeld für den Namen des Ausschlussbereichs. Dieser Name wird in der Tabelle im Fenster Ausschlüsse nach Prozessen angezeigt.
Pfad des auszuschließenden Prozesses	Vollständiger Pfad des Prozesses, den Sie von der Untersuchung ausschließen möchten. Bei der Angabe des Pfades können Masken verwendet werden. Das Eingabefeld darf nicht leer sein.
Auf untergeordnete Prozesse anwenden	Untergeordnete Prozesse des ausgeschlossenen Prozesses, der durch den Parameter **Pfad des auszuschließenden Prozesses** angegeben ist, 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 Anwendung. 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. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Prozess von der Untersuchung durch die Verhaltensanalyse ausschließen	Das Kontrollkästchen aktiviert oder deaktiviert den Ausschluss eines Prozesses von der Untersuchung, während die Komponente "Verhaltensanalyse" ausgeführt wird. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Prozess aus den Telemetriedaten von MDR und EDR Expert (on-premise) ausschließen	Mit diesem Kontrollkästchen wird die Ausnahme des Prozesses von den Telemetriedaten aktiviert oder deaktiviert, die von den Komponenten MDR und EDR Expert (on-premise) erfasst werden. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Exploit-Prävention

In der Verwaltungskonsole können Sie die Exploit-Prävention in den Richtlinieneigenschaften konfigurieren (**Erweiterter Schutz** → **Verhaltensanalyse**).

Einstellungen der Komponente „Exploit-Prävention"

Parameter	Description
Exploit-Prävention aktivieren	Das Kontrollkästchen aktiviert oder deaktiviert die Komponente "Exploit-Prävention". Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Exploit-Prävention	Über die Schaltfläche **Konfigurieren** öffnet sich das Fenster **Ausnahmen aus der Exploit-Prävention**, in dem Sie die Untersuchungsausnahmen der Komponente Exploit-Prävention konfigurieren können.
Aktion beim Erkennen eines Exploits	Die von der Anwendung ausgeführte Aktion, wenn ein Exploit gefunden wird: • **Blockieren** (Standardwert). Die Anwendung blockiert die schädlichen Vorgänge des Exploits und zeichnet Informationen darüber im Ereignisprotokoll auf. • **Informieren**. Die Anwendung blockiert keine Vorgänge von Exploits, sondern zeichnet nur Informationen über die Erkennung eines Exploits im Ereignisprotokoll auf.

Fenster "Ausnahmen aus der Exploit-Prävention"

In diesem Fenster können Sie den Ausschluss von Objekten aus der Exploit-Prävention konfigurieren. Die Anwendung untersucht die angegebenen Objekte nicht. Standardmäßig ist die Liste der Objekte leer.

Parameter der Ausnahme aus der Exploit-Prävention

Parameter	Description
Werte bei Vererbung vereinen	Das Kontrollkästchen aktiviert oder deaktiviert die Vereinigung der Liste, wenn diese von untergeordneten Richtlinien geerbt wird. Wenn das Kontrollkästchen aktiviert ist, werden die Elemente der übergeordneten Richtlinienliste in den untergeordneten Richtlinien angezeigt und die Elemente können der untergeordneten Richtlinienliste hinzugefügt werden. Bei deaktiviertem Kontrollkästchen werden die Listenelemente beim Vererben von Richtlinieneinstellungen nicht vereinigt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der Anwendung angewendet wird.
Bedrohungsname	Name der Bedrohung, die von der Untersuchung ausgeschlossen werden soll.
Pfad zur Datei oder zum Verzeichnis	Vollständiger Pfad zur Datei oder dem Verzeichnis, die von der Untersuchung ausgeschlossen werden.
Hash-Summer der Datei	Hash-Summe der Datei, die von der Untersuchung ausgeschlossen wird.
Kommentar	Ein Kommentar zur Untersuchungsausnahme.

Standardmäßig ist die Tabelle mit den Ausnahmen leer. Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Fenster "Ausnahme aus der Exploit-Prävention"

In diesem Fenster können Sie eine Ausnahme aus der Untersuchung durch die Komponente "Exploit-Prävention" hinzufügen oder konfigurieren.

Parameter der Ausnahme aus der Exploit-Prävention

Parameter	Description
Bedrohungsname verwenden	Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung der Ausnahme aus der Objektuntersuchung basierend auf dem Namen der im Objekt erkannten Bedrohung. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Bedrohungsname	Eingabefeld für den Namen der im Objekt erkannten Bedrohung. 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. Den vollständigen Namen der im Objekt gefundenen Bedrohung finden Sie im Protokoll der Anwendung oder auf der Website https://threats.kaspersky.com . Dieses Feld ist verfügbar, wenn das Kontrollkästchen **Bedrohungsname verwenden** aktiviert ist.

Parameter	Description
Hash-Summe der Datei verwenden	Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung der Ausnahme aus der Dateiuntersuchung basierend auf deren Hash-Summe. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Typ der Hash-Summe der Datei	In der Dropdown-Liste können Sie den Typ der Hash-Summe der Datei auswählen, anhand dessen die Datei von der Untersuchung ausgeschlossen werden soll. • **MD5**. • **SHA256**. Die Dropdown-Liste ist verfügbar, wenn das Kontrollkästchen **Hash-Summe der Datei verwenden** aktiviert ist.
Hash-Summe der Datei	Eingabefeld für die Hash-Summe der Datei, anhand derer die Datei aus der Untersuchung ausgeschlossen werden soll. Das Feld ist verfügbar, wenn das Kontrollkästchen **Hash-Summe der Datei verwenden** aktiviert ist.
Pfad zur Datei oder zum Verzeichnis verwenden	Das Kontrollkästchen aktiviert oder deaktiviert das Ausschließen einer Datei, in der eine Bedrohung erkannt wurde, anhand ihres Pfads von der Untersuchung. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Pfad zur Datei oder zum Verzeichnis	Eingabefeld für den Pfad zur Datei oder zum lokalen Verzeichnis, die aus der Untersuchung ausgeschlossen werden. Bei der Angabe des Pfades können Sie die Zeichen * und ? verwenden. Dieses Feld ist verfügbar, wenn das Kontrollkästchen **Pfad zur Datei oder zum Verzeichnis verwenden** aktiviert ist.
Kommentar	Eingabefeld für einen Kommentar (optional).
Diesen Ausschluss verwenden	Dieses Kontrollkästchen aktiviert oder deaktiviert die Verwendung dieser Ausnahme während der Ausführung der Anwendung. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Schutz vor Verschlüsselung

In der Verwaltungskonsole können Sie die Einstellungen für den Schutz vor Verschlüsselung in den Eigenschaften der Richtlinie verwalten (**Erweiterter Schutz → Schutz vor Verschlüsselung**).

Einstellungen der Komponente „Schutz vor Verschlüsselung“

Parameter	Description
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.
Ausnahmen	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Ausnahmebereiche** geöffnet. In diesem Fenster können Sie eine Liste mit Bereichen festlegen, die von der Untersuchung ausgeschlossen werden sollen.
Ausnahmen 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.

Parameter	Description
Name des Bereichs	Name des Untersuchungsbereichs
Path	Der Pfad zu dem zu untersuchenden Verzeichnis.
Status	Der Status gibt an, ob die Anwendung 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 aufgeführt sind. Wenn Sie für ein Unterverzeichnis Sicherheitseinstellungen anpassen möchten, die sich von den Sicherheitseinstellungen des übergeordneten Verzeichnisses unterscheiden, 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 aufgeführt sind. Wenn Sie für ein Unterverzeichnis Sicherheitseinstellungen anpassen möchten, die sich von den Sicherheitseinstellungen des übergeordneten Verzeichnisses unterscheiden, müssen Sie das Unterverzeichnis in der Tabelle über dem übergeordneten Verzeichnis platzieren.

Die Schaltfläche ist verfügbar, wenn ein Bereich in der Tabelle ausgewählt wurde.

Durch Klicken auf die Schaltfläche **Löschen** wird der ausgewählte Bereich von Untersuchungen 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.

Parameter	Description
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 Anwendung. 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. Dieses 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 Masken verwendet werden. Das Feld darf nicht leer sein.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der Anwendung 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.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Fenster "Schutzeinstellungen"

Schutzeinstellungen

Parameter	Description
Aktion beim Erkennen einer Verschlüsselung:	Aktion, die Kaspersky Endpoint Security ausführt, wenn es eine schädliche Verschlüsselung erkennt: • **Informieren** Sie den Benutzer. 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 vertrauenswürdige Geräte 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 Anwendung 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 2147483647. Standardwert: 30.

Fenster "Ausschlussbereiche"

Das Fenster enthält die Ausschlussbereiche einer Untersuchung. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden.

Einstellungen des Ausschlussbereichs

Parameter	Description
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Path	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der Anwendung angewendet wird.

Standardmäßig ist die Tabelle mit den Ausschlussbereichen leer. Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

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 „Neuer Ausnahmebereich“

- In diesem Fenster können Sie einen neuen Bereich mit Untersuchungsausschlüssen hinzufügen oder anpassen.

Einstellungen des Ausschlussbereichs

Parameter	Description
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 Anwendung. Wenn das Kontrollkästchen aktiviert ist, schließt die App diesen Bereich während ihrer Ausführung von der Untersuchung aus. Wenn das Kontrollkästchen deaktiviert ist, schließt die Anwendung diesen Bereich während ihrer Ausführung in die Untersuchung ein. Sie können diesen Bereich zu einem späteren Zeitpunkt ausschließen, indem Sie das Kontrollkästchen aktivieren. Dieses 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** für lokale Verzeichnisse. • **Mounted** für eingebundene Verzeichnisse. • **Alle remote-mounted** für alle Remote-Verzeichnisse, die auf dem Gerät über das Samba- und das NFS-Protokoll eingebunden sind.
	Wenn in der Dropdown-Liste der Dateisysteme **Mounted** ausgewählt ist, können Sie in der Dropdown-Liste rechts das Protokoll für den Remote-Zugriff auswählen: • **NFS** für Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** für Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** für Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind.
	Wenn in der Dropdown-Liste der Dateisysteme **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu einem Verzeichnis angeben, das Sie dem Ausnahmebereich hinzufügen möchten. Bei der Angabe des Pfades können Sie Masken und Tags 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 der Dateisysteme der Typ **Mounted** ausgewählt ist und in der Dropdown-Liste rechts das Element **Benutzerdefiniert** ausgewählt ist.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der Anwendung 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.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

So verwenden Sie Tags

Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Wobei gilt:

`<id>` ist die Container-ID.

`<name>` ist ein Containername

`<path to local directory>` ist der Pfad zum lokalen Verzeichnis.

Sie können auch eindeutige Kombinationen von Tags verwenden: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` und `[image-name:<name>]/path to local directory>`.

Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert.

Beispielsweise:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden.

Fenster "Ausnahmen nach Maske"

Sie können eine Namensmaske verwenden, um Untersuchungsausnahmen für Objekte zu 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 **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).

Sie können die Vereinigung der Ausschlusslisten aktivieren, wenn diese von untergeordneten Richtlinien geerbt werden. Um die Listenelemente zu vereinigen, muss das Kontrollkästchen **Werte beim Vererben vereinigen aktiviert** sein. Wenn das Kontrollkästchen aktiviert ist, werden die Elemente der übergeordneten Richtlinienliste in den untergeordneten Richtlinien angezeigt und die Elemente können der untergeordneten Richtlinienliste hinzugefügt werden. Bei deaktiviertem Kontrollkästchen werden die Listenelemente beim Vererben von Richtlinieneinstellungen nicht vereinigt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Kaspersky Security Network

In der Verwaltungskonsole können Sie die Verwendung von Kaspersky Security Network in Kaspersky Endpoint Security in den Eigenschaften der Richtlinie (**Erweiterter Schutz → Kaspersky Security Network**) konfigurieren.

Sie können den Text der **Erklärung zu Kaspersky Security Network** im Fenster „Erklärung zu Kaspersky Security Network“ lesen. Dieses Fenster kann durch Klicken auf den Link **Kaspersky Security Network-Erklärung** geöffnet werden.

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.

Einstellungen für „Kaspersky Security Network“

Parameter	Description
Erklärung zu Kaspersky Security Network	Durch Klicken auf diesen Link wird das Fenster **Erklärung zu Kaspersky Security Network** geöffnet. 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	Im *Cloud-Modus* verwendet Kaspersky Endpoint Security eine schlanke Version der Antiviren-Datenbanken, wodurch die Belastung des Arbeitsspeichers des Computers ungefähr halbiert wird. 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 Anwendungsdatenbanken aktiviert oder deaktiviert. Die Einstellung wird nur angewendet, wenn die Anwendung im Standard-Modus verwendet wird.
Administrationsserver als KSN-Proxyserver verwenden	Wenn das Kontrollkästchen aktiviert ist, interagiert Kaspersky Endpoint Security über den KSN Proxyservice des Administrationsservers mit den KSN-Servern. Dieses Kontrollkästchen ist standardmäßig aktiviert. Die Einstellung wird nur angewendet, wenn die Anwendung im Standard-Modus verwendet wird. Im Light Agent-Modus kann das Programm mit der KSN-Infrastruktur nur über einen KSN-Proxyserver kommunizieren.

Parameter	Description
KSN-Server verwenden, wenn KSN-Proxyserver nicht verfügbar	Wenn das Kontrollkästchen aktiviert ist, interagiert Kaspersky Endpoint Security direkt mit den KSN-Servern, wenn der KSN Proxy-Service nicht verfügbar ist. Dieses Kontrollkästchen ist standardmäßig aktiviert. Das Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Administrationsserver als KSN-Proxyserver verwenden** aktiviert ist. Die Einstellung wird nur angewendet, wenn die Anwendung 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“

Parameter	Description
Mehr Info	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 Online-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 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.
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“

Parameter	Description
Hiermit bestätige ich, dass ich die Bedingungen der Erklärung zu Kaspersky Security Network vollständig gelesen und verstanden habe und diese 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. Diese Option ist verfügbar, wenn Sie im Fenster **Einstellungen für 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. Diese Option ist verfügbar, wenn Sie im Fenster **Einstellungen für Kaspersky Security Network** die Option **standardmäßiger KSN-Modus** oder **erweiterter KSN-Modus** ausgewählt haben.

Erklärung zu Kaspersky Private Security Network

In diesem Fenster können Sie den Text der Erklärung zu Kaspersky Security Network lesen und deren Bedingungen akzeptieren.

Einstellungen für „Kaspersky Security Network“

Parameter	Description
Hiermit bestätige ich, dass ich die Bedingungen der Erklärung zu Kaspersky Security Network vollständig gelesen und verstanden habe und diese 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 Private 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.

Schutz vor modifizierten USB-Geräten

In der Verwaltungskonsole können Sie die Einstellungen für den Schutz vor Web-Bedrohungen in den Eigenschaften der Richtlinie verwalten (**Basisschutz → Schutz vor BadUSB-Angriffen**).

Parameter der Komponente zum Schutz vor BadUSB-Angriffen

Parameter	Description
Schutz vor BadUSB-Angriffen aktivieren	Dieses Kontrollkästchen aktiviert oder deaktiviert die Komponente "Schutz vor BadUSB-Angriffen". Die Komponente ist standardmäßig deaktiviert.
Maximale Anzahl der Autorisierungsversuche für USB-Geräte	Das USB-Gerät wird automatisch gesperrt, wenn der Autorisierungscode zu oft falsch eingegeben wurde. Mögliche Werte: 1 bis 10. Wenn Sie beispielsweise 5 Versuche zur Eingabe des Autorisierungscodes erlauben, wird das USB-Gerät nach dem fünften erfolglosen Eingabeversuch durch die Anwendung blockiert. Kaspersky Endpoint Security zeigt den Zeitpunkt, an dem das USB-Gerät blockiert wurde. Nach Ablauf dieses Zeitraums haben Sie erneut fünf Versuche, den Autorisierungscode einzugeben.
Wenn maximale Anzahl der Autorisierungsversuche erreicht wird, Gerät blockieren für (Min.)	Die Dauer, für die ein USB-Gerät nach einer bestimmten Anzahl erfolgloser Eingabeversuche des Autorisierungscodes gesperrt wird. Die möglichen Werte liegen zwischen 1 und 180 (Minuten).
Verwendung der Bildschirmtastatur zur Autorisierung von USB-Geräten verbieten	Wenn der Schalter aktiviert ist, verbietet das Programm die Verwendung einer Bildschirmtastatur für die Autorisierung eines USB-Geräts, von dem aus der Autorisierungscode nicht eingegeben werden kann.
Verwendung eines Strichcodes zur Autorisierung von USB-Geräten verbieten	Wenn dieser Umschalter aktiviert ist, lässt das Programm die Verwendung eines Barcodes zur Autorisierung eines USB-Geräts nicht zu, mit dem kein Autorisierungscode eingegeben werden kann.

Schutz von Verbindungen und Kommunikation über das Netzwerk

Schutz vor E-Mail-Bedrohungen

In der Verwaltungskonsole können Sie die Einstellungen für den Schutz vor Web-Bedrohungen in den Eigenschaften der Richtlinie verwalten (**Basisschutz → Schutz vor E-Mail-Bedrohungen**).

Einstellungen der Komponente „Schutz vor E-Mail-Bedrohungen“

Parameter	Description
Schutz vor E-Mail-Bedrohungen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Komponente "Schutz vor E-Mail-Bedrohungen". Die Komponente ist standardmäßig aktiviert.
Konfigurieren (Schutzeinstellungen)	Durch Klicken auf die Schaltfläche öffnet sich das Fenster **Einstellungen des Schutzes vor E-Mail-Bedrohungen**, in dem Sie den Schutzbereich des Schutzes vor E-Mail-Bedrohungen und die Einstellungen für die Untersuchung zusammengesetzter Dateien konfigurieren können.
Konfigurieren (Anlagenfilterung)	Durch Klicken auf die Schaltfläche öffnet sich das Fenster **Anlagenfilterung**, in dem Sie die Filterung von E-Mail-Anhängen konfigurieren können.
Heuristische Analyse verwenden **Stufe der heuristischen Analyse**	Dieses Kontrollkästchen aktiviert oder deaktiviert die Verwendung der heuristischen Analyse. Im Rahmen der Untersuchung von Dateien auf schädlichen Code führt die heuristische Analyse die Anweisungen in ausführbaren Dateien aus. Die Anzahl der ausgeführten Anweisungen hängt von der ausgewählten Stufe der heuristischen Analyse ab. Die Stufe der heuristischen Analyse reguliert das Verhältnis zwischen der Gründlichkeit der Suche nach neuen Bedrohungen, der Belastung der Betriebssystemressourcen und der Dauer der heuristischen Analyse. Standardmäßig ist die heuristische Analyse mit ausgewählter mittlerer Analysestufe aktiviert.
Aktionen beim Erkennen von Bedrohungen	Aktion, die vom Schutz vor E-Mail-Bedrohungen bei Erkennung einer Bedrohung in E-Mail-Nachrichten ausgeführt wird: • **Desinfizieren. Löschen, wenn Desinfektion fehlschlägt**. Wenn ein infiziertes Objekt in einer eingehenden Nachricht erkannt wird, versucht die Anwendung, das Objekt zu desinfizieren. Der Benutzer erhält die Nachricht mit ungefährlichem Anhang. Wenn die Desinfektion fehlschlägt, löscht die Anwendung das infizierte Objekt. Die Anwendung fügt dem Nachrichtenbetreff eine Information über die ausgeführte Aktion hinzu, z. B. *[Nachricht wurde verarbeitet] <Nachrichtenbetreff>*. Diese Aktion ist standardmäßig ausgewählt. • **Desinfizieren. Blockieren, wenn Desinfektion fehlschlägt**. Wenn ein infiziertes Objekt in einer eingehenden Nachricht erkannt wird, versucht die Anwendung, das Objekt zu desinfizieren. Der Benutzer erhält die Nachricht mit ungefährlichem Anhang. Wenn das Objekt nicht desinfiziert werden konnte, fügt die Anwendung dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit ihrem ursprünglichen Anhang. • **Blockieren**. Wenn ein infiziertes Objekt in einer eingehenden Nachricht erkannt wird, fügt die Anwendung dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit ihrem ursprünglichen Anhang. Diese Einstellung gilt nicht für ausgehende Nachrichten. Wenn in einer ausgehenden Nachricht ein infiziertes Objekt entdeckt wird, blockiert die Anwendung den Versand der Nachricht.

Fenster "Einstellungen des Schutzes vor E-Mail-Bedrohungen"

In diesem Fenster können Sie den Schutzbereich für den Schutz vor E-Mail-Bedrohungen und die Einstellungen der Untersuchung von zusammengesetzten Dateien konfigurieren.

Einstellungen des Schutzes vor E-Mail-Bedrohungen

Parameter	Description
Schutzbereich	Der *Schutzbereich* umfasst die Objekte, die von der Komponente während ihrer Ausführung untersucht werden: eingehende und ausgehende Nachrichten oder nur eingehende Nachrichten. Standardmäßig ist die Option **Ein- und ausgehende Nachrichten** ausgewählt.
Angehängte Archive untersuchen	Aktiviert oder deaktiviert die Untersuchung angehängter Archive. Untersucht Archive der Formate ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE und mehr. Die Anwendung durchsucht Archive nicht nur nach Dateiendung, sondern auch nach Format. Bei der Untersuchung von Archiven entpackt die Anwendung diese rekursiv. Dadurch können Bedrohungen in verschachtelten Archiven (d. h. Archive in Archiven) erkannt werden. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Angehängte Dateien von Office-Anwendungen untersuchen	Aktiviert oder deaktiviert die Untersuchung angehängter Office-Dateien. Die Anwendung untersucht Office-Dateien, die kleiner als 1 MB sind, unabhängig vom Status des Kontrollkästchens. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Parameter	Description
Archive nicht untersuchen, wenn größer als (MB)	Wenn das Kontrollkästchen aktiviert ist, schließt die Komponente zum Schutz vor E-Mail-Bedrohungen jene E-Mail-Anhänge, die größer als der angegebene Wert sind, von der Untersuchung aus. Wenn dieses Kontrollkästchen deaktiviert ist, untersucht der Schutz vor E-Mail-Bedrohungen Archive beliebiger Größe, die an E-Mail-Nachrichten angehängt sind. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Archive nicht länger untersuchen als (Sek.)	Wenn das Kontrollkästchen aktiviert ist, wird die Zeit für die Untersuchung der Archive, die an E-Mail-Nachrichten angehängt sind, auf die eingegebene Dauer beschränkt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Fenster "Anhangsfilter"

In diesem Fenster können Sie die Filterung von Anhängen für E-Mail-Nachrichten einrichten.

Parameter des Anhangsfilters

Parameter	Description
Filter nicht anwenden	Wenn diese Option ausgewählt ist, filtert der Schutz vor E-Mail-Bedrohungen keine an E-Mail-Nachrichten angehängten Dateien.
Anhänge der angegebenen Typen umbenennen	Wenn diese Option ausgewählt ist, ersetzt der Schutz vor E-Mail-Bedrohungen das letzte Zeichen der Dateierweiterung von angehängten Dateien der angegebenen Typen durch einen Unterstrich (z. B. attachment.doc_). Wenn ein Benutzer die Datei öffnen möchte, muss er sie daher zunächst umbenennen. Standardmäßig ausgewählt.
Anhänge der angegebenen Typen löschen	Wenn diese Option ausgewählt ist, entfernt der Schutz vor E-Mail-Bedrohungen Anhänge mit den angegebenen Dateitypen aus E-Mail-Nachrichten. Die Dateitypen der Anhänge, die umbenannt oder aus der E-Mail-Nachricht entfernt werden sollen, können Sie in der Liste der Dateimasken angeben.
Werte bei Vererbung zusammenführen	Das Kontrollkästchen aktiviert oder deaktiviert die Vereinigung der Liste, wenn diese von untergeordneten Richtlinien geerbt wird. Wenn das Kontrollkästchen aktiviert ist, werden die Elemente der übergeordneten Richtlinienliste in den untergeordneten Richtlinien angezeigt und die Elemente können der untergeordneten Richtlinienliste hinzugefügt werden. Bei deaktiviertem Kontrollkästchen werden die Listenelemente beim Vererben von Richtlinieneinstellungen nicht vereinigt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Tabelle der Anhangstypen	Die Tabelle zeigt die Typen der Anhänge, die umbenannt oder E-Mail-Nachrichten entfernt werden sollen. Sie können die Anhangstypen über gleichnamigen Schaltflächen hinzufügen, bearbeiten und löschen.

Schutz vor Web-Bedrohungen

In der Verwaltungskonsole können Sie die Einstellungen für den Schutz vor Web-Bedrohungen in den Richtlinieneigenschaften (**Basisschutz → Schutz vor Web-Bedrohungen**) konfigurieren.

Einstellungen der Komponente „Schutz vor Web-Bedrohungen"

Parameter	Description
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.

Parameter	Description
Aktion beim Fund einer Bedrohung	Aktion, die von der Anwendung 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 ermöglicht das Herunterladen dieses Objekts auf das Gerät. Dabei protokolliert die Anwendung 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 von Webadressen können Sie Masken verwenden. IP-Adressen können nicht mit Masken beschrieben werden. Standardmäßig ist die Liste leer. Sie können die Webadressen in der Liste hinzufügen, bearbeiten und löschen.

Nützliche Artikel

So geben Sie Masken an

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

Parameter	Description
Schädliche Objekte erkennen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Überprüfung von Links gegen Datenbanken mit bösartigen Webadressen. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Phishing-Links erkennen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Überprüfung von Links gegen Datenbanken mit Phishing-Adressen. Dieses 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.

Parameter	Description
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 Netzwerkbedrohungen

In der Verwaltungskonsole können Sie die Einstellungen für den Schutz vor Netzwerkbedrohungen in den Richtlinieneigenschaften verwalten (**Basisschutz → Schutz vor Netzwerkbedrohungen**).

Einstellungen der Komponente "Schutz vor Netzwerkbedrohungen"

Parameter	Description
Schutz vor Netzwerkbedrohungen aktivieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Komponente "Schutz vor Netzwerkbedrohungen". Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Aktion beim Fund einer Bedrohung	Zu ergreifende Maßnahmen, wenn eine Netzwerkaktivität erkannt wird, die auf Netzwerkangriffe hinweist: • **Informieren** Sie den Benutzer. Die Anwendung 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 Hosts aktivieren	Dieses Kontrollkästchen aktiviert und deaktiviert das Blockieren der Netzwerkaktivität, wenn ein versuchter Netzwerkangriff erkannt wird. Dieses 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 Kaspersky Endpoint Security die Netzwerkaktivität von diesem Gerät aus. Mögliche Werte sind ganze Zahlen zwischen 1 und 32768. Standardwert: 60.
Ausnahmen	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, über die das Fenster Ausnahmen geöffnet wird, in dem Sie eine Liste von IP-Adressen angeben können. Netzwerkangriffe von diesen IP-Adressen werden nicht blockiert.

Fenster "Ausnahmen"

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. Sie können IP-Adressen in den Formaten IPv4 und IPv6 eingeben.

Firewall-Verwaltung

In der Verwaltungskonsole können Sie die Einstellungen für die Firewall-Verwaltung in den Richtlinieneigenschaften konfigurieren (**Basisschutz → Firewall-Verwaltung**).

Einstellungen der Komponente "Firewall-Verwaltung"

Parameter	Description
Firewall-Verwaltung aktivieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Komponente "Firewall-Verwaltung". Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Netzwerkpaketregeln	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Netzwerkpaketregeln** geöffnet. In diesem Fenster können Sie die Netzwerkpaketregeln konfigurieren, die von der Komponente "Firewall-Verwaltung" angewendet werden, wenn eine versuchte Netzwerkverbindung erkannt wird.
Verfügbare Netzwerke	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Verfügbare Netzwerke** geöffnet. 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). • **Blockieren** von Netzwerkverbindungen.
Eingehende Pakete	In dieser Dropdown-Liste können Sie eine Aktion auswählen, die für eingehende Pakete ausgeführt wird: • Eingehende Pakete **erlauben** (Standardwert). • **Blockieren** eingehender Pakete.
Immer Erlaubnisregeln für Administrationsagent-Ports hinzufügen	Dieses Kontrollkästchen aktiviert oder deaktiviert das automatische Hinzufügen von Erlaubnisregeln für Ports des Administrationsagenten. Dieses 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

Parameter	Description
Name	Name der Netzwerkpaketregel
Aktion	Aktion, welche die Komponente "Firewall-Verwaltung" bei Erkennen von Netzwerkaktivität ausführt.
Lokale Adresse	Netzwerkadressen der Geräte, auf denen die Anwendung 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 Anwendung die Aktionen der Netzwerkpaketregel protokolliert. Wenn in der Spalte **Ja** angegeben ist, protokolliert die Anwendung die Aktionen der Netzwerkpaketregel. Wenn in der Spalte **Nein** angegeben ist, protokolliert die Anwendung 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.

Fenster "Netzwerkpaketregel hinzufügen"

In diesem Fenster können Sie die Einstellungen der hinzuzufügenden Netzwerkpaketregel anpassen.

Einstellungen der Netzwerkpaketregel

Parameter	Description
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 dieses Element ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" nur eingehende Pakete. • **Eingehend** Wenn dieses Element ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" nur eingehende Verbindungen. • **Eingehende/Ausgehende** (Standardwert). Wenn dieses Element ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" sowohl eingehende als auch ausgehende Verbindungen. • **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" nur ausgehende Pakete. • **Ausgehend** Wenn dieses Element ausgewählt ist, überwacht die Komponente "Firewall-Verwaltung" nur ausgehende Verbindungen.
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 in der Dropdown-Liste **Protokoll** als Datenübertragungsprotokoll **ICMP** oder **ICMPv6** ausgewählt ist.
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 in der Dropdown-Liste **Protokoll** als Datenübertragungsprotokoll **ICMP** oder **ICMPv6** ausgewählt ist.
Remote-Ports	Sie können die Portnummer oder den Bereich aus 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 nur angezeigt, wenn in der Dropdown-Liste **Protokoll** als Datenübertragungsprotokoll **TCP** oder **UDP** ausgewählt ist.
Lokale Ports	Sie können die Portnummer oder den Bereich aus 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 nur angezeigt, wenn in der Dropdown-Liste **Protokoll** als Datenübertragungsprotokoll **TCP** oder **UDP** ausgewählt ist.
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 oder Adressbereich**. Wenn diese Option ausgewählt ist, kontrolliert die Netzwerkregel jene Netzwerkpakete, die von Remote-Geräten mit den in der Tabelle darunter angegebenen IP-Adressen, gesendet und empfangen wurden. Durch Klick auf die Schaltfläche **Hinzufügen** über der Tabelle wird das Fenster **IP-Adressen hinzufügen** geöffnet. Dort können Sie die IP-Adresse des Geräts, die Netzwerkadresse oder den IP-Adressbereich angeben. • **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 Anwendung 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 Anwendung Kaspersky Endpoint Security und beliebigen IP-Adressen gesendet und empfangen werden. • **Angegebene Adresse oder Adressbereich**. Wenn diese Option ausgewählt ist, kontrolliert die Netzwerkregel die Netzwerkadressen von Geräten, auf denen Kaspersky Endpoint Security installiert ist und die Netzwerkpakete senden und empfangen können. Diese Netzwerkadressen sind in der folgenden Tabelle angegeben. Durch Klick auf die Schaltfläche **Hinzufügen** über der Tabelle wird das Fenster **IP-Adressen hinzufügen** geöffnet. Dort können Sie die IP-Adresse des Geräts, die Netzwerkadresse oder den IP-Adressbereich angeben.

Parameter	Description
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 "IP-Adressen hinzufügen"

In diesem Fenster können Sie die IP-Adresse des Geräts, die Netzwerkadresse oder den IP-Adressbereich angeben.

Wenn Sie mehrere Adressen angeben, geben Sie jede Adresse in einer neuen Zeile ein, um sie einfacher kopieren zu können.

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

Parameter	Description
IP-Adresse	Netzwerk-IP-Adresse.
Netzwerktyp	Netzwerktyp (**Öffentliches Netzwerk**, **Lokales Netzwerk** oder **Vertrauenswürdiges Netzwerk**).

Sie können verfügbare Netzwerke hinzufügen, bearbeiten und löschen.

Fenster "Netzwerkverbindung"

In diesem Fenster können Sie eine Netzwerkverbindung anpassen, die von der Komponente "Firewall-Verwaltung" überwacht werden soll.

Netzwerkverbindung

Parameter	Description
IP-Adresse	Eingabefeld für die Netzwerk-IP-Adresse.
Netzwerktyp	Sie können den Netzwerktyp wählen: • **Öffentliches Netzwerk** • **Lokales Netzwerk** • **Vertrauenswürdiges Netzwerk**

Sicherheitskontrolle

Gerätekontrolle

In der Verwaltungskonsole können Sie die Einstellungen der Gerätekontrolle in den Richtlinieneigenschaften (**Sicherheitskontrolle → Gerätekontrolle**) verwalten.

Einstellungen der „Gerätekontrolle“

Parameter	Description
Gerätekontrolle aktivieren	Dieser Schalter aktiviert bzw. deaktiviert die Komponente Gerätekontrolle. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Vertrauenswürdige Geräte	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Vertrauenswürdige Geräte** geöffnet. In diesem Fenster können Sie ein Gerät zur Liste der vertrauenswürdigen Geräte hinzufügen.
Ausführungsmodus der Gerätekontrolle	Ausführungsmodus der Anwendung 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 für den erkannten Versuch, auf ein Gerät zuzugreifen. • **Blockieren** (Standardwert). Wenn Sie diese Option auswählen, wendet Kaspersky Endpoint Security den für das Gerät oder die Schnittstelle angegebenen Zugriffsmodus an.
Einstellungen der Komponente "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.
Anfordern des temporären Zugriffs erlauben	Wenn dieses Kontrollkästchen aktiviert ist, kann der Benutzer in der grafischen Benutzeroberfläche des Programms oder über die Befehlszeile temporären Zugriff auf das blockierte Gerät anfordern.
Benachrichtigungsvorlagen	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Nachrichtenvorlagen** geöffnet.

Fenster Vertrauenswürdige Geräte

Die Tabelle enthält eine Liste der vertrauenswürdigen Geräte. Standardmäßig die Tabelle leer.

Einstellungen eines vertrauenswürdigen Geräts

Parameter	Description
Geräte-ID	ID eines vertrauenswürdigen Geräts.
Gerätename	Name eines vertrauenswürdigen Geräts.
Typ des Geräts	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.
Benutzer oder Gruppe	Name des Benutzers oder der Benutzergruppe, für die das Gerät als vertrauenswürdig gilt.
Kommentar	Kommentar zu einem vertrauenswürdigen Gerät.

Mithilfe der Schaltfläche **Hinzufügen** können Sie Geräte auf folgende Arten zur Liste der vertrauenswürdigen Geräte hinzufügen:

- Indem Sie die Geräte-ID oder eine Maske der ID angeben (**Hinzufügen → Gerät mittels ID oder Maske hinzufügen**).
- Indem Sie das gewünschte Gerät aus der Liste der auf verwalteten Geräten erkannten Geräte auswählen (**Hinzufügen → Gerät aus der Liste mit den auf dem Client-Gerät gefundenen Geräten auswählen**).
- Indem Sie das gewünschte Gerät aus der Liste der in den Ereignissen der Gerätekontrolle in Kaspersky Security Center erkannten Geräte auswählen (**Hinzufügen → Gerät basierend auf Ereignissen hinzufügen**).

Sie können vertrauenswürdige Geräte in der Tabelle bearbeiten und löschen.

Sie können die Liste der hinzugefügten Geräte auch in eine Datei exportieren, indem Sie auf die Schaltfläche **Erweitert → Ausgewählte exportieren** oder **Erweitert → Alle exportieren** klicken, und eine Liste mit Geräten aus einer Datei im JSON-Format importieren, indem Sie auf die Schaltfläche **Erweitert → Importieren** klicken.

Für den Import stehen drei Modi zur Verfügung:

- **Mit bestehenden vereinigen** – Vereinigt die Listen vertrauenswürdiger Geräte beim Import. Wenn die Datei bereits einen Eintrag für ein Gerät mit derselben ID enthält, werden die Parameter des vorhandenen Eintrags geändert. Einträge für Geräte, die zuvor nicht in der Liste enthalten waren, werden hinzugefügt.
- **Zu bestehenden hinzufügen** – Erweitert die Liste vertrauenswürdiger Geräte beim Import. Es werden nur die Einträge für Geräte hinzugefügt, die zuvor nicht in der Liste enthalten waren.
- **Bestehende ersetzen** – Ersetzt die Liste vertrauenswürdiger Geräte. Die bestehende Liste vertrauenswürdiger Geräte wird durch die Liste aus der Datei ersetzt.

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

Parameter	Description
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).
Benutzern und/oder Benutzergruppen Zugriff gewähren	Feld, das den Namen eines Benutzers und/oder einer Gruppe von Benutzern anzeigt, für die das Gerät vertrauenswürdig ist. Standardmäßig ist **\Everyone** (alle Benutzer) angegeben.
Konfigurieren	Durch Anklicken der Schaltfläche öffnet sich das Fenster **Zugriff auf ein vertrauenswürdiges Gerät**.

Fenster "Geräte an Client-Geräten"

In diesem Fenster können Sie ein Gerät zu einer Liste vertrauenswürdiger Geräte hinzufügen, indem Sie es aus der Liste mit der auf dem verwalteten Client-Gerät gefundenen Geräten auswählen.

Informationen zu vorhandenen Geräten sind nur verfügbar, wenn eine aktive Richtlinie erstellt wurde 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 inaktive Richtlinie erstellen, ist die Liste leer.

Hinzufügen von Geräten aus der Liste der Geräte, die auf den Client-Geräten gefunden wurden

Parameter	Description
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).
Typ des Geräts	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 Anwendung nach Geräten mit den angegebenen Parametern. Die Suchergebnisse werden in der Tabelle darunter angezeigt.
Liste der gefundenen Geräte	Folgende Spalten sind in der Tabelle enthalten: • **Name des Client-Geräts** – Der Name des Client-Geräts, mit dem das gefundene Gerät verbunden ist. • **Gerätetyp** – Der Typ des gefundenen Geräts (z. B. Festplatte oder Smartcard-Reader). • **Gerätename** – Name des gefundenen Geräts. • **Geräte-ID** – ID des gefundenen Geräts.

Fenster "Liste von Geräten basierend auf den Ereignissen der Gerätekontrolle"

In diesem Fenster können Sie eine Liste der Geräte erstellen, die in den Ereignissen der Gerätekontrolle in Kaspersky Security Center erkannt wurden. Geräte aus dieser Liste können Sie anschließend der Liste der vertrauenswürdigen Geräte hinzufügen.

Sie können ein oder mehrere Geräte zur Liste der vertrauenswürdigen Geräte hinzufügen.

Informationen zu Geräten sind verfügbar, wenn die Gerätekontrolle aktiviert ist, 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 inaktive Richtlinie erstellen, ist die Liste leer.

Hinzufügen von Geräten aus der Liste der Geräte, die in den Ereignissen in Kaspersky Security Center erkannt wurden

Parameter	Description
Ereignistypen	Mithilfe der Kontrollkästchen können Sie die Typen der Ereignisse der Gerätekontrolle, die an Kaspersky Security Center gesendet werden, auswählen. Die Liste enthält Geräte, die in Ereignissen des angegebenen Typs erkannt wurden. Standardmäßig sind alle Kontrollkästchen aktiviert.
Administrationsgruppe	Feld zur Eingabe des Namens der Administrationsgruppe, welche die Client-Geräte enthält, mit denen die erkannten Geräte verbunden sind. Die Liste enthält nur Geräte, die mit Client-Geräten der angegebenen Administrationsgruppe verbunden sind. Die teilweise Eingabe des Gruppennamens ist möglich. Standardmäßig sind in der Liste Geräte enthalten, die mit Client-Geräten aller Administrationsgruppen verbunden sind.
Zeitraum der Ereignisgenerierung	Wählen Sie mithilfe der Dropdown-Liste den Zeitraum aus, in dem die Ereignisse aufgetreten sind. Die Liste enthält Geräte, die in Ereignissen erkannt wurden, die während des angegebenen Zeitraums an Kaspersky Security Center gesendet wurden. Standardmäßig sind in der Liste Geräte enthalten, die in den Ereignissen des letzten Monats erkannt wurden.
Gerätesuche	Wenn Sie auf diese Schaltfläche klicken, sucht die Anwendung nach Geräten mit den angegebenen Parametern. Die Suchergebnisse werden in der Tabelle darunter angezeigt.
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. • **Verbunden am** – Datum, an dem das erkannte Gerät verbunden wurde. • **Administrationsgruppe** – Name der Administrationsgruppe, die das Client-Gerät enthält, mit dem das erkannte Gerät verbunden ist.

Parameter	Description
Kommentar	Eingabefeld für den Kommentar zum Gerät, das Sie zur Liste der vertrauenswürdigen Geräte hinzufügen möchten (optional).
Benutzern und/oder Benutzergruppen Zugriff gewähren	Feld, das den Namen eines Benutzers und/oder einer Gruppe von Benutzern anzeigt, für die das Gerät vertrauenswürdig ist. Standardmäßig ist **\Everyone** (alle Benutzer) angegeben.
Konfigurieren	Durch Anklicken der Schaltfläche öffnet sich das Fenster **Zugriff auf ein vertrauenswürdiges Gerät**.

Fenster "Zugriff auf ein vertrauenswürdiges Gerät"

In diesem Fenster können Sie den Zugriff für Benutzer oder Benutzergruppen auf ein ausgewähltes vertrauenswürdiges Gerät konfigurieren.

Zugriff auf ein vertrauenswürdiges Gerät

Parameter	Description
Benutzer und/oder Benutzergruppen	Liste der Benutzer und Gruppen, für die das hinzugefügte Gerät als vertrauenswürdig gilt. Standardmäßig enthält die Tabelle das Element **\Everyone** (alle Benutzer). Sie können Benutzergruppen hinzufügen, bearbeiten und löschen.

Fenster "Benutzer oder Gruppe"

In diesem Fenster können Sie einen Benutzer oder eine Gruppe von Benutzern angeben, für welche das Gerät als vertrauenswürdig gilt.

Einstellungen eines vertrauenswürdigen Geräts

Parameter	Description
Typ	Der **Benutzer** oder die **Gruppe**, für die das Gerät als vertrauenswürdig gilt.
Benutzer oder Gruppe	Der Name eines lokalen Benutzers oder des Domänenbenutzers (ohne Angabe des vollständigen Namens mit Domäne [wenn diese Formatangabe im System zulässig ist] oder im Format <Domänenname>\<Benutzername> oder <Benutzername>@<Domänenname>) oder der Name einer Gruppe von Benutzern, für welche das Gerät als vertrauenswürdig gilt.

Fenster "Gerätetyp"

In diesem Fenster können Sie den Zugriffsmodus für verschiedene Gerätetypen anpassen.

Zugriffsmodus für Gerätetypen

Parameter	Description
Typ des Geräts	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 Punkte 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. • **Nach Regeln** – Erlaubt oder blockiert den Zugriff auf Geräte gemäß Zugriffsregel und Zeitplan. Dieser Menüpunkt ist nur für Geräte verfügbar, die für das Speichern von Daten vorgesehen sind (Festplatten, Wechseldatenträger, Disketten, CD/DVD-Laufwerke). • **Nur lesen** – Erlaubt nur Lesezugriff auf Geräte des ausgewählten Typs. Dieser Menüpunkt ist nur für Geräte verfügbar, die für das Speichern von Daten vorgesehen sind (Festplatten, Wechseldatenträger, Disketten, CD/DVD-Laufwerke).

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

Parameter	Description
Benutzer und/oder Benutzergruppen	Eine Liste der Benutzer und Gruppen, für die Sie Zugriffszeitpläne konfigurieren können. Standardmäßig enthält die Tabelle das Element **\Everyone** (alle Benutzer). Sie können Benutzergruppen hinzufügen, bearbeiten und löschen.
Gerätezugriffsregeln	Diese Tabelle enthält Zugriffszeitpläne für Benutzer und Benutzergruppen. Sie 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 **\Everyone** ausgewählt), wenn für diesen Gerätetyp der Zugriff über einen Verbindungsbus aktiviert ist. Für ausgewählte Benutzer können Sie Zugriffszeitpläne hinzufügen, ändern und löschen. Der Zeitplan **Standard** kann weder geändert noch gelöscht werden.

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	Description
Typ	**Benutzer** oder **Gruppe**, für welchen bzw. welche die Regel gilt.
Benutzer oder Gruppe	Name des lokalen Benutzers oder der Benutzergruppe, für die die Regel gilt.

Fenster "Zugriffszeitplan"

In diesem Fenster können Sie die Zugriffszeitpläne für Geräte anpassen.

Zeitplan für Gerätezugriff

Parameter	Description
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 "Verbindungsbusse"

In diesem Fenster können Sie den Zugriffsmodus für Bus-Verbindungen konfigurieren.

Zugriffsmodus für Bus-Verbindungen

Parameter	Description
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 Punkte 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.

Web-Kontrolle

In der Verwaltungskonsole können Sie die Einstellungen der Web-Kontrolle in den Richtlinieneigenschaften (**Sicherheitskontrolle → Web-Kontrolle**) verwalten.

Einstellungen der Komponente „Web-Kontrolle"

Parameter	Description
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 verwenden** 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.
	Sie können auch eine Liste mit Regeln aus einer Datei importieren, indem Sie auf **Erweitert → Importieren** klicken, und die Liste der hinzugefügten Regeln in eine Datei exportieren, indem Sie auf **Zusätzlich → Ausgewählte exportieren** oder **Zusätzlich → Alle exportieren** klicken. 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 Anwendung den Zugriff auf Webressourcen regelt, die keinen anderen Regeln unterliegen, auswählen: • **Allow** (Standardwert) – Gewährt Zugriff auf die Webressourcen. • **Block** – Verbietet den Zugriff auf die Webressourcen.
Benachrichtigungsvorlagen	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Nachrichtenvorlagen** geöffnet.

Fenster "Regel der Web-Kontrolle"

In diesem Fenster können Sie die Einstellungen der Regel für den Zugriff auf die Webressourcen anpassen.

Parameter	Description
Regelname	Eingabefeld für den Namen der Zugriffsregel auf die Webressourcen. Der Relgename muss eindeutig sein.
Diese Regel verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Verwendung dieser Regel während der Ausführung der Anwendung. 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. Dieses 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 dieses Element ausgewählt ist, wird die Schaltfläche **Auswählen** verfügbar. Durch Klicken auf diese Schaltfläche wird das Fenster **Auswahl der Inhaltskategorie** geöffnet. • **Nach Datentypkategorien**. Wenn dieses Element ausgewählt ist, wird die Schaltfläche **Auswählen** verfügbar. Durch Klicken auf diese Schaltfläche wird das Fenster **Auswahl der Datentypkategorie** geöffnet. • **Nach Inhalts- und Datentypkategorien**. Wenn dieses Element ausgewählt ist, werden die Schaltflächen **Auswählen** verfügbar. Durch Klicken auf diese Schaltflächen werden Fenster geöffnet, in denen Sie die erforderlichen Kategorien auswählen 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 dieses Element ausgewählt ist, wird die Schaltfläche **Adressen auswählen** verfügbar. Durch Klicken auf diese Schaltfläche wird das Fenster **Adressen auswählen** geöffnet, in dem Sie die erforderlichen Adressen der Webressourcen auswählen 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 dieses Element ausgewählt ist, wird die Schaltfläche **Benutzer auswählen** verfügbar. Durch Klicken auf diese Schaltfläche wird das Fenster **Benutzer auswählen** 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. • **<Name 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: • **Allow** (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.

Fenster "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 erforderlichen Kategorien.

Standardmäßig sind alle Kontrollkästchen deaktiviert.

Wenn Sie die Kontrollkästchen für alle untergeordneten Inhaltskategorien aktivieren, wird das Kontrollkästchen neben der Haupt-Inhaltskategorie, welche die untergeordneten Inhaltskategorien enthält, nicht automatisch aktiviert.

Fenster "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 erforderlichen Kategorien.

Standardmäßig sind alle Kontrollkästchen deaktiviert.

Fenster "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.

Fenster "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.

Wenn Sie der Gruppenliste in diesem Fenster eine neue Adressgruppe hinzufügen möchten, öffnen Sie das Fenster **Adressgruppe hinzufügen**, indem Sie auf die Schaltfläche **Hinzufügen** klicken, die sich oberhalb der Tabelle befindet.

Standardmäßig die Tabelle leer.

Fenster "Adressgruppe 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.

Fenster "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.

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.

Parameter	Description
Typ	**Benutzer** oder **Gruppe**, für welchen bzw. welche die Regel gilt.
Benutzer oder Gruppe	Name des Benutzers oder der Benutzergruppe, auf welche die Regel angewendet wird.

Fenster "Zugriffszeitplan"

In diesem Fenster können Sie die den Zugriffszeitplan für die Webressource anpassen.

Zugriffszeitplan für die Webressourcen.

Parameter	Description
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.

Programmkontrolle

In der Verwaltungskonsole können Sie die Einstellungen der Programmkontrolle in den Richtlinieneigenschaften verwalten (**Sicherheitskontrolle** → **Programmkontrolle**).

Einstellungen für die Komponente „Programmkontrolle"

Parameter	Description
Programmkontrolle aktivieren	Dieses Kontrollkästchen aktiviert die Komponente zur Programmkontrolle. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Aktion beim Versuch, eine Anwendung zu starten	Aktion, die Kaspersky Endpoint Security ausführen soll, wenn ein Versuch erkannt wird, eine Anwendung 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 Anwendung zu starten, die den Regelbedingungen entspricht.
Modus der App-Kontrolle	Ausführungsmodus der Komponente zur Programmkontrolle: • **Allow-Liste**. Bei Auswahl dieser Option verbietet Kaspersky Endpoint Security allen Benutzern den Start aller Anwendungen, außer der in den Regeln der Programmkontrolle angegebenen. • **Deny-Liste** (Standardwert). Bei Auswahl dieser Option erlaubt Kaspersky Endpoint Security allen Benutzern den Start aller Anwendungen, außer der in den Regeln der Programmkontrolle angegebenen.
Regeln der Programmkontrolle	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Regeln der Programmkontrolle** geöffnet.
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 Anwendung nur die in der Richtlinie angegebenen Regeln angewendet. • **Regeln aus der Richtlinie zu den lokalen Regeln hinzufügen** (Standardwert) Wenn dieser Eintrag ausgewählt ist, werden Regeln, die in der Richtlinie konfiguriert wurden, zusammen mit lokalen Regeln, die auf dem geschützten Gerät konfiguriert wurden, angewendet.

Fenster "Regeln der App-Kontrolle"

Die Tabelle **Regeln der Programmkontrolle** enthält die Regeln, die von der Komponente zur Programmkontrolle verwendet werden. Standardmäßig ist die Tabelle mit den Regeln der Programmkontrolle leer.

Einstellungen der Regeln der App-Kontrolle

Parameter	Description
Name der Kategorie	Der Name der App-Kategorie, die in der Regel verwendet wird.
Status	Der Status der Regel der Programmkontrolle: • *Aktiviert* – Die Regel ist aktiviert und wird während der Ausführung der Programmkontrolle angewendet. • *Deaktiviert* – Die Regel ist deaktiviert und wird während der Ausführung der Programmkontrolle nicht angewendet. • *Test* – Die Aufgabe zur Programmkontrolle erlaubt das Starten von Anwendungen, die den Regelbedingungen entsprechen, nimmt aber Informationen über den Start dieser Anwendungen im Bericht auf. Den Status einer Regel können Sie im Fenster **Regel hinzufügen** ändern.

Sie können Regeln der Programmkontrolle hinzufügen, bearbeiten und löschen.

Fenster "Regel hinzufügen"

In diesem Fenster können Sie die Einstellungen der Regel für die App-Kontrolle anpassen.

Regel für die App-Kontrolle hinzufügen

Parameter	Description
Description	Regelbeschreibung für die App-Kontrolle
Regelstatus	In dieser Dropdown-Liste können Sie einen Status für die Regel der Programmkontrolle auswählen: • *Aktiviert* – Die Regel ist aktiviert und wird während der Ausführung der Programmkontrolle angewendet. • *Deaktiviert* – Die Regel ist deaktiviert und wird während der Ausführung der Programmkontrolle nicht angewendet. • *Test* – Die Aufgabe zur Programmkontrolle erlaubt das Starten von Anwendungen, die den Regelbedingungen entsprechen, nimmt aber Informationen über den Start dieser Anwendungen im Bericht auf.
Kategorie	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Programmkategorien** geöffnet.

Parameter	Description
Benutzer und ihre Berechtigungen	Diese Tabelle enthält eine Liste mit Namen der Benutzer oder Benutzergruppen, für welche die Regel für die Programmkontrolle 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 Programmkontrolle gilt. • **Zugriff** – Zugriffstyp: Starten der Anwendung **erlauben** oder **blockieren**. Sie können Benutzergruppen hinzufügen, bearbeiten und löschen.

Fenster "Programmkategorien"

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

Parameter	Description
Name der Kategorie	Liste der hinzugefügten Kategorien der Programmkontrolle.
Hinzufügen	Durch Klicken auf die Schaltfläche wird der Assistent zum Erstellen einer Kategorie gestartet. Folgen Sie den Anweisungen. Weitere Informationen über das Erstellen von Kategorien finden Sie in der Hilfe zu Kaspersky Security Center.
Ändern	Diese Schaltfläche öffnet das Fenster mit den Kategorie-Eigenschaften, in dem Sie die Einstellungen der Kategorie anpassen können. Die Kategorie **Golden Image (lokal)** kann nicht geändert werden.

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

Parameter	Description
Typ	**Benutzer** oder **Gruppe**, für welchen bzw. welche die Regel gilt.
Benutzer oder Gruppe	Name des Benutzers oder der Benutzergruppe, für welche die Regel für die Programmkontrolle gilt.
Access	Zugriffstyp: Starten der Anwendung **erlauben** oder **blockieren**.

Inventar

In der Verwaltungskonsole von Kaspersky Security Center können Sie mithilfe der Aufgabe *Inventarisierung* eine Inventarisierung der Anwendungen auf einem geschützten Gerät durchführen.

Sie können Benutzeraufgaben für die Inventarisierung erstellen und ausführen. Sie können die Untersuchungseinstellungen verwalten, indem Sie die Einstellungen der Aufgaben bearbeiten.

In der Datenbank der Anwendung 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

Parameter	Description
Aktion mit der Kategorie "Golden Image" nach Aufgabenabschluss	In der Dropdown-Liste können Sie die Aktion auswählen, die Kaspersky Endpoint Security nach Abschluss der Inventarisierungsaufgabe mit der Programmkategorie „Golden Image“ ausführen soll: • **Keine Änderungen** – die Programmkategorie „Golden Image“ nach Abschluss der Inventarisierung nicht ändern. Dieser Wert ist standardmäßig ausgewählt. • **Aktualisieren oder erstellen (falls nicht vorhanden)** – Programme, die die Inventarisierungsaufgabe auf dem Gerät erkennt, zur Kategorie „Golden Image“ hinzufügen. Wenn die Kategorie nicht vorhanden ist, wird sie erstellt. Wenn eine Kategorie existiert, wird die Liste der darin enthaltenen Anwendungen aktualisiert. • **Löschen** – die Programmkategorie „Golden Image“ leeren. Die Kategorie wird sofort nach dem Start der Aufgabe geleert, ohne dass eine Inventarisierung der Dateien auf dem Gerät durchgeführt wird. Sie können die Kategorie „Golden Image“ in den Regeln der Programmkontrolle verwenden.
Alle ausführbaren Dateien untersuchen	Das Kontrollkästchen aktiviert und deaktiviert die Untersuchung von ausführbaren Dateien. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Binärdateien untersuchen	Das Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Binärdateien (mit den Erweiterungen .elf, .java und .pyc). Dieses Kontrollkästchen ist standardmäßig aktiviert.
Skripte untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Skripten. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Bereiche der Inventarisierung	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Untersuchungsbereiche** geöffnet.

Im Abschnitt **Ausnahmen** 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

Parameter	Description
Name des Bereichs	Name des Untersuchungsbereichs
Path	Der Pfad zu dem zu untersuchenden Verzeichnis.
Status	Der Status gibt an, ob die Anwendung diesen Bereich während ihrer Ausführung untersucht.

Sie können Elemente in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.

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

Parameter	Description
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. Dieses 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 Masken verwendet werden. Das Feld darf nicht leer sein.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der Anwendung während der Ausführung der Aufgabe untersucht werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Abschnitt "Ausnahmen"

Einstellungen der Ausnahmen von der Untersuchung

Einstellungsgruppe	Description
Ausschlussbereiche	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster Ausnahmebereiche geöffnet. In diesem Fenster können Sie eine Liste mit Bereichen festlegen, die von der Überwachung ausgeschlossen werden sollen.

Fenster "Ausschlussbereiche"

Das Fenster enthält die Ausschlussbereiche einer Untersuchung. Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden.

Einstellungen des Ausschlussbereichs

Parameter	Description
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Path	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status zeigt an, ob dieser Ausschluss bei der Ausführung der Anwendung angewendet wird.

Standardmäßig ist die Tabelle mit den Ausschlussbereichen leer. Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

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 „Neuer Ausnahmebereich“

In diesem Fenster können Sie einen Bereich mit Untersuchungsausschlüssen für die Inventarisierungsaufgabe hinzufügen und bearbeiten.

Einstellungen des Ausschlussbereichs

Parameter	Description
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 Anwendung diesen Bereich während ihrer Ausführung aus. Wenn das Kontrollkästchen deaktiviert ist, schließt die Anwendung diesen Bereich während ihrer Ausführung ein. Im Folgenden können Sie diesen Bereich aus der Untersuchung ausnehmen, indem Sie das Kontrollkästchen aktivieren. Dieses 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 Masken verwendet werden. Das Feld darf nicht leer sein.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der Anwendung von der Untersuchung ausgeschlossen werden. Sie können Masken hinzufügen, bearbeiten und löschen.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Überwachung der System-Integrität

In der Verwaltungskonsole können Sie die Einstellungen für die Überwachung der Systemintegrität in den Eigenschaften der Richtlinie konfigurieren (**Sicherheitskontrolle → Überwachung der Systemintegrität**).

Einstellungen der Überwachung der Systemintegrität

Parameter	Description
Überwachung der Systemintegrität aktivieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Überwachung der System-Integrität. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Überwachungsbereiche	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Wenn Sie auf diese Schaltfläche klicken, wird das Fenster **Untersuchungsbereiche** geöffnet.
Überwachungsausnahmen	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Ausnahmebereiche** geöffnet.
Ausnahmen 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

Parameter	Description
Werte bei Vererbung vereinen	Das Kontrollkästchen aktiviert oder deaktiviert die Vereinigung der Liste, wenn diese von untergeordneten Richtlinien geerbt wird. Wenn das Kontrollkästchen aktiviert ist, werden die Elemente der übergeordneten Richtlinienliste in den untergeordneten Richtlinien angezeigt und die Elemente können der untergeordneten Richtlinienliste hinzugefügt werden. Bei deaktiviertem Kontrollkästchen werden die Listenelemente beim Vererben von Richtlinieneinstellungen nicht vereinigt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Name des Bereichs	Name des Überwachungsbereichs.
Path	Pfad zu dem durch das Programm geschützten Verzeichnis.
Status	Der Status gibt an, ob die Anwendung diesen Bereich während ihrer Ausführung untersucht.

Sie können Elemente in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.

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

Parameter	Description
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 Anwendung. Wenn das Kontrollkästchen aktiviert ist, überwacht die Anwendung diesen Bereich während der Ausführung. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich von der Anwendung während der Ausführung nicht überwacht. Sie können diesen Bereich zu einem späteren Zeitpunkt zu den Betriebseinstellungen der Komponente hinzufügen, indem Sie das Kontrollkästchen aktivieren. Dieses 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 Anwendung während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen.

Fenster "Ausschlussbereiche"

Die Fenster enthält die Ausschlussbereiche der Komponente "Überwachung der System-Integrität". Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden.

Einstellungen des Bereichs mit Ausschlüsse von der Überwachung

Parameter	Description
Werte bei Vererbung vereinen	Das Kontrollkästchen aktiviert oder deaktiviert die Vereinigung der Liste, wenn diese von untergeordneten Richtlinien geerbt wird. Wenn das Kontrollkästchen aktiviert ist, werden die Elemente der übergeordneten Richtlinienliste in den untergeordneten Richtlinien angezeigt und die Elemente können der untergeordneten Richtlinienliste hinzugefügt werden. Bei deaktiviertem Kontrollkästchen werden die Listenelemente beim Vererben von Richtlinieneinstellungen nicht vereinigt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Path	Pfad zum Verzeichnis, das von der Überwachung ausgenommen ist.
Status	Der Status gibt an, ob die Anwendung diesen Bereich während der Ausführung der Aufgabe von der Untersuchung ausschließt.

Standardmäßig ist die Tabelle mit den Ausschlussbereichen leer. Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Sie können auch eine Liste mit Ausschlussbereichen aus einer Datei importieren, indem Sie auf die Schaltfläche **Importieren** klicken und die Liste der Ausschlussbereiche über die Schaltflächen **Exportieren** in eine Datei im JSON-Format exportieren. Beim Importieren wird Ihnen vorgeschlagen, entweder die Liste der Ausnahmebereiche zu ersetzen oder die Ausnahmebereiche zu einer bestehenden Liste hinzuzufügen.

Fenster „Neuer Ausnahmebereich“

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

Parameter	Description
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 Anwendung. Wenn das Kontrollkästchen aktiviert ist, schließt die Anwendung diesen Bereich während der Ausführung der Komponente von der Überwachung aus. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich von der Anwendung während der Ausführung der Komponente überwacht. Im Folgenden können Sie diesen Bereich von der Überwachung ausschließen, indem Sie das Kontrollkästchen aktivieren. Dieses 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 Anwendung 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 **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 Überwachung 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 "Ausnahmen nach Maske"

Sie können den Ausschluss von Objekten von der Überwachung anhand einer Namensmaske konfigurieren. Die Anwendung 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 **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 Überwachung 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).

Sie können die Ausnahmeliste auch mithilfe der Schaltfläche **Importieren** aus einer Datei importieren und mithilfe der Schaltfläche **Exportieren** in eine JSON-Datei exportieren. Beim Importieren wird Ihnen vorgeschlagen, entweder die Liste der Ausnahmen zu ersetzen oder die Ausnahmen zu einer bestehenden Liste hinzuzufügen.

Sie können die Vereinigung der Ausschlusslisten aktivieren, wenn diese von untergeordneten Richtlinien geerbt werden. Um die Listenelemente zu vereinigen, muss das Kontrollkästchen **Werte beim Vererben vereinigen aktiviert** sein. Wenn das Kontrollkästchen aktiviert ist, werden die Elemente der übergeordneten Richtlinienliste in den untergeordneten Richtlinien angezeigt und die Elemente können der untergeordneten Richtlinienliste hinzugefügt werden. Bei deaktiviertem Kontrollkästchen werden die Listenelemente beim Vererben von Richtlinieneinstellungen nicht vereinigt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Prüfung der Systemintegrität

In der Verwaltungskonsole können Sie mithilfe der Aufgabe *Prüfung der Systemintegrität* Prüfungen der Systemintegrität durchführen.

Sie können benutzerdefinierte Aufgaben zur Prüfung der Systemintegrität erstellen und starten. Sie können die Untersuchungseinstellungen verwalten, indem Sie die Einstellungen der Aufgaben bearbeiten.

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

Parameter	Description
Baseline bei jedem Aufgabenstart neu erstellen	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 Anwendung 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	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Wenn Sie auf diese Schaltfläche klicken, wird das Fenster **Untersuchungsbereiche** geöffnet.

In den Abschnitten **Ausnahmebereiche** in den Eigenschaften der Prüfung der Systemintegrität können Sie Ausnahmen von der Überwachung und Ausnahmen nach Maske definieren.

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

Parameter	Description
Name des Bereichs	Name des Überwachungsbereichs.
Path	Pfad zu dem durch das Programm geschützten Verzeichnis.
Status	Der Status gibt an, ob die Anwendung diesen Bereich während ihrer Ausführung untersucht.

Sie können Elemente in der Tabelle hinzufügen, bearbeiten, löschen, nach oben verschieben und nach unten verschieben.

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

Parameter	Description
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 Anwendung. Wenn das Kontrollkästchen aktiviert ist, überwacht die Anwendung diesen Bereich während der Ausführung. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich von der Anwendung während der Ausführung nicht überwacht. Sie können diesen Bereich zu einem späteren Zeitpunkt zu den Betriebseinstellungen der Komponente hinzufügen, indem Sie das Kontrollkästchen aktivieren. Dieses 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 Masken verwendet werden. 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 Anwendung während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske * (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Abschnitt "Ausnahmen"

Einstellungen der Ausnahmen von der Untersuchung

Einstellungsgruppe	Description
Überwachungsausnahmen	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Ausnahmebereiche** geöffnet. In diesem Fenster können Sie eine Liste mit Bereichen festlegen, die von der Überwachung ausgeschlossen werden sollen.
Ausnahmen 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

Parameter	Description
Name des Ausschlussbereichs	Name des Ausschlussbereichs.
Path	Pfad zum Verzeichnis, das von der Untersuchung ausgenommen ist.
Status	Der Status gibt an, ob die Anwendung diesen Bereich während der Ausführung der Aufgabe von der Untersuchung ausschließt.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Fenster „Neuer Ausnahmebereich“

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

Parameter	Description
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 Anwendung. Wenn das Kontrollkästchen aktiviert ist, schließt die Anwendung diesen Bereich während der Ausführung der Aufgabe von der Überwachung aus. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich von der Anwendung während der Ausführung der Aufgabe überwacht. Im Folgenden können Sie diesen Bereich von der Überwachung ausschließen, indem Sie das Kontrollkästchen aktivieren. Dieses 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 Masken verwendet werden. 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 Anwendung 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 **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).

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Fenster "Ausnahmen nach Maske"

Sie können den Ausschluss von Objekten von der Überwachung anhand einer Namensmaske konfigurieren. Die Anwendung 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 **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).

Lokale Aufgaben

Aufgabenverwaltung

In der Verwaltungskonsole können Sie in den Richtlinieneigenschaften die Berechtigung zum Anzeigen und Verwalten von Aufgaben festlegen (**Lokale Aufgaben** → **Aufgabenverwaltung**).

Einstellungen für die Aufgabenverwaltung

Parameter	Description
Verwendung lokaler Aufgaben erlauben	Dieses Kontrollkästchen erlaubt oder verbietet Benutzern, lokale, in der Anwendung Kaspersky Endpoint Security erstellte Aufgaben anzuzeigen und diese Aufgaben auf verwalteten Client-Geräten zu verwalten. Wenn diese Option aktiviert ist, können Benutzer Aufgaben in der grafischen Oberfläche der Anwendung und in der Befehlszeile konfigurieren und ausführen. Wenn das Kontrollkästchen deaktiviert ist, können die Aufgaben nicht lokal verwendet werden. Es werden keine lokalen Aufgaben per Zeitplan ausgeführt. Aufgaben können weder in der grafischen Oberfläche der Anwendung noch in der Befehlszeile gestartet oder konfiguriert werden. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Benutzern das Anzeigen und Verwalten von KSC-Aufgaben erlauben	Dieses Kontrollkästchen erlaubt oder verbietet Benutzern, über Kaspersky Security Center erstellte Aufgaben anzuzeigen und diese Aufgaben auf Client-Geräten zu verwalten. Wenn das Kontrollkästchen aktiviert ist, werden Aufgaben, die über Kaspersky Security Center erstellte wurden, in der grafischen Oberfläche der Anwendung angezeigt. Benutzer können diese Aufgaben über die grafische Oberfläche der Anwendung und über die Befehlszeile starten und stoppen. Wenn das Kontrollkästchen deaktiviert wird, ist sowohl das Anzeigen als auch die Verwaltung von Aufgaben, die über Kaspersky Security Center erstellt wurden, weder in der grafischen Oberfläche der Anwendung noch in der Befehlszeile möglich. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Schutz vor komplexen Bedrohungen und gezielten Angriffen

Integration von Kaspersky Managed Detection and Response

In der Verwaltungskonsole können Sie die MDR-Komponente aktivieren oder deaktivieren und die MDR-BLOB-Datei in den Richtlinieneigenschaften hochladen (**Detection and Response → Managed Detection and Response**).

Einstellungen der Integration mit MDR

Parameter	Description
Managed Detection and Response aktivieren	Das Kontrollkästchen aktiviert oder deaktiviert die MDR-Komponente, die für die Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response erforderlich ist. Die Komponente ist standardmäßig deaktiviert. Wenn Sie die MDR-Komponente aktivieren und Kaspersky Security Network deaktiviert ist oder im Standardmodus ausgeführt wird, werden Sie aufgefordert, die Nutzungsbedingungen von Kaspersky Security Network zu akzeptieren, um den erweiterten Modus von Kaspersky Security Network zu aktivieren. Wenn das Ändern der KSN-Einstellungen durch die übergeordnete Richtlinie verboten wird, erscheint eine Fehlermeldung und die MDR-Komponente wird nicht aktiviert.
Laden	Diese Schaltfläche öffnet ein Microsoft Windows-Standardfenster, in dem Sie die MDR-BLOB-Datei zum Hochladen auswählen können. Diese Aktion ist obligatorisch, wenn Sie Mandanten haben oder wenn Sie die MDR-Komponente mithilfe der MDR-BLOB-Datei aktiviert haben.

Die BLOB-Datei befindet sich in einem ZIP-Archiv der MDR-Konfigurationsdatei, die im Lieferumfang von Kaspersky Managed Detection and Response enthalten ist.

Durch das Hochladen der BLOB-Datei erklären Sie sich damit einverstanden, automatisch Daten von einem Gerät mit installiertem Kaspersky Endpoint Security zur Verarbeitung an Kaspersky zu übermitteln. Laden Sie die Datei nicht hoch, 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 in Kaspersky Endpoint Detection and Response (on-premises)

In der Verwaltungskonsole können Sie die Komponente EDR Expert (on-premise) aktivieren oder deaktivieren und die Einstellungen für die Integration des Programms Kaspersky Endpoint Security mit der Komponente Kaspersky Endpoint Detection and Response (KATA) in den Richtlinieneigenschaften (**Detection and Response → EDR Expert (on-premise)**) verwalten.

Wenn in der Web Console für die Komponente EDR Expert (on-premise) die Option **Endpoint Detection and Response Expert (Version 8.0 und höher)** ausgewählt ist, d. h. der Integrationsmodus EDR Expert (on-premise) ausgewählt ist, zeigt die Verwaltungskonsole eine Warnung an, und die Einstellungen für die Integration mit Kaspersky Endpoint Detection and Response (KATA) sind nicht verfügbar. Sie können in der Web Console den Integrationsmodus ändern.

Einstellungen der Integration in Kaspersky Endpoint Detection and Response (on-premises)

Parameter	Description
Endpoint Detection and Response Expert (on-premises) aktivieren	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Komponente EDR Expert (on-premise), die die Integration mit Kaspersky Endpoint Detection and Response (KATA) bereitstellt. Die Komponente ist standardmäßig deaktiviert.
Ausführungsprävention für Objekte aktivieren	Dieses Kontrollkästchen aktiviert bzw. deaktiviert Regeln von EDR Expert (on-premise) für die Ausführungsprävention für Objekte.
KATA-Server	Wenn Sie auf die Schaltfläche **Konfigurieren** klicken, wird ein Fenster geöffnet. In diesem können Sie die Verbindung zu den KATA-Servern konfigurieren und eine Liste der Server anzeigen, zu denen eine Verbindung konfiguriert ist.
Einstellungen für die Verbindung mit Servern	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.

Verbindung mit den KATA-Servern konfigurieren

Die Tabelle enthält eine Liste der Parameter für die Verbindung mit den KATA-Servern. 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.

Einstellungen für die Verbindung mit Servern

Parameter	Description
Adresse	Die IP-Adresse (IPv4 oder IPv6) oder der vollqualifizierte Domänenname (FQDN) des KATA-Integrationsservers kann angegeben werden. Um sicherzustellen, dass die Kommunikation mit dem Server nicht unterbrochen wird, wenn die Anwendung 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`.

Allgemeine Einstellungen für die Verbindung mit KATA-Servern konfigurieren

In diesem Fenster können Sie die allgemeinen Einstellungen für Verbindungen mit KATA-Servern konfigurieren.

Einstellungen für die Verbindung mit dem KATA-Server

Einstellung	Description
Synchronisierungsanfrage an KATA-Server senden alle (Min.)	Häufigkeit des Sendens von Synchronisierungsanfragen an den KATA-Server in Minuten. Der Standardwert ist: `5`.
Maximale Wartezeit für die Verbindung zum Server (Sek.)	Die maximale Wartezeit auf eine Verbindung mit dem KATA-Server in Sekunden. Der Standardwert ist: `10`.

Einstellung	Description
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	Dieses Kontrollkästchen aktiviert oder deaktiviert das Senden von Daten über Ereignisse auf Geräten (Telemetriedaten) an den KATA-Server. Standardmäßig ist das Senden von Telemetriedaten aktiviert.

Serverzertifikat	Die Einstellungsgruppe enthält Schaltflächen zum Hinzufügen und Entfernen eines Serverzertifikats:
	• **Hinzufügen** – Öffnet ein Fenster zum Hinzufügen eines Serverzertifikats. Die Schaltfläche wird angezeigt, wenn noch kein Serverzertifikat hinzugefügt wurde.
	In dem Fenster zum Hinzufügen des Zertifikats können Sie das Zertifikat eines KATA-Servers auf eine der folgenden Arten hinzufügen:
	  • Geben Sie im Feld **Aus Datei hinzufügen** den Pfad zu der Zertifikatsdatei an, die das Zertifikat im DER- oder PEM-Format enthält. Mit der Schaltfläche **Durchsuchen** wird ein Standardfenster für die Dateiauswahl geöffnet.
	  • Kopieren Sie den Inhalt der Zertifikatsdatei in das Feld **Zertifikatdaten einfügen**.
	Wenn ein Serverzertifikat hinzugefügt wurde, wird das Serverzertifikat auf Seiten von Kaspersky Endpoint Security überprüft. Dies erhöht die Sicherheit der Verbindung.
	• **Löschen** – Entfernt ein zuvor hinzugefügtes Serverzertifikat. Diese Schaltfläche wird angezeigt, wenn ein Serverzertifikat hinzugefügt wurde.

Erweiterter Schutz der Verbindung	Die Einstellungsgruppe enthält Oberflächenelemente, mit denen die Zwei-Wege-Authentifizierung konfiguriert wird. Diese dient einer zusätzlichen Absicherung der Verbindung: • **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 Zwei-Wege-Authentifizierung aktiviert sein. • **Hinzufügen** – Öffnet ein Fenster zum Hinzufügen eines Client-Zertifikats, um die Verbindung mit dem KATA-Server zusätzlich abzusichern. Die Schaltfläche wird angezeigt, wenn das Kontrollkästchen **Zwei-Wege-Authentifizierung verwenden** aktiviert ist und noch kein Client-Zertifikat hinzugefügt wurde. Um ein Client-Zertifikat hinzuzufügen, geben Sie im Fenster zum Hinzufügen des Zertifikats den Pfad zu dem Krypto-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. Geben Sie anschließend das Kennwort für das Client-Zertifikat im Feld **Kennwort für Crypto-Container** ein. Das Feld ist ein Pflichtfeld. Wenn Sie versuchen, die Einstellungen ohne Eingabe eines Kennworts zu speichern, wird eine Fehlermeldung angezeigt. Wenn das Kennwort korrekt ist, wird die Schaltfläche **OK** aktiv. Sie können die Einstellungen speichern. • **Löschen** – Entfernt ein zuvor hinzugefügtes Client-Zertifikat. Die Schaltfläche wird nur angezeigt, wenn ein Client-Zertifikat hinzugefügt wurde.

Datenübertragung an die KATA-Server konfigurieren

In diesem Fenster können Sie die Einstellungen für die Datenübertragung an die KATA-Server konfigurieren.

Einstellungen zur Datenübertragung an die KATA-Server

Parameter	Description
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.

Parameter	Description
Maximale Anzahl an Ereignissen pro Stunde	Maximale Anzahl an Ereignissen pro Stunde Der Standardwert ist: `3000`.
Prozentuale Überschreitung der Beschränkung der Ereignisanzahl	Prozentuale Überschreitung der Beschränkung der Ereignisanzahl: 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 Network Detection and Response (KATA)

In der Verwaltungskonsole können Sie die Komponente NDR (KATA) aktivieren oder deaktivieren und die Einstellungen für die Integration des Programms Kaspersky Endpoint Security mit der Komponente Kaspersky Network Detection and Response (KATA) in den Eigenschaften der Richtlinie verwalten (**Detection and Response → Network Detection and Response (KATA)**).

Parameter für die Integration mit Kaspersky Network Detection and Response (KATA)

Parameter	Description
Network Detection and Response (KATA) aktivieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Komponente NDR (KATA). Die Komponente ist standardmäßig deaktiviert.
NDR-Server	Wenn Sie auf die Schaltfläche **Konfigurieren** klicken, wird ein Fenster geöffnet. In diesem können Sie die Verbindung zu den NDR-Servern konfigurieren und eine Liste der Server anzeigen, zu denen eine Verbindung konfiguriert ist.
Einstellungen für die Verbindung mit Servern	Wenn Sie auf die Schaltfläche **Konfigurieren** klicken, wird ein Fenster geöffnet, in dem Sie bei Verbindung mit den NDR-Servern die allgemeinen Einstellungen für die Verbindung mit den NDR-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 NDR-Server konfigurieren können.

Verbindung mit den NDR-Servern konfigurieren

Die Tabelle enthält eine Liste der Parameter für die Verbindung mit den NDR-Servern. 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 NDR-Server hinzufügen.
- Bereits konfigurierte Verbindungseinstellungen ändern oder löschen.
- Eine Liste mit den konfigurierten Verbindungseinstellungen exportieren oder importieren.

Einstellungen für die Verbindung mit Servern

Parameter	Description
Adresse	Die IP-Adresse (IPv4 oder IPv6) oder der vollqualifizierte Domänenname (FQDN) des NDR-Integrationsservers kann angegeben werden. Der Standardwert ist: `127.0.0.1`.
Port	Port für die Verbindung zum NDR-Server. Der Standardwert ist: `443`.

Allgemeine Einstellungen für die Verbindung mit NDR-Servern konfigurieren

In diesem Fenster können Sie die allgemeinen Verbindungseinstellungen mit den NDR-Servern konfigurieren.

Einstellungen für die Verbindung mit den NDR-Servern

Parameter	Description
Synchronisierungsanfrage an NDR-Server senden alle (Min.)	Häufigkeit des Sendens von Synchronisierungsanfragen an den NDR-Server in Minuten. Der Standardwert ist: `5`.
Maximale Wartezeit für die Verbindung zum Server (Sek.)	Die maximale Wartezeit auf eine Verbindung mit dem NDR-Server in Sekunden. Der Standardwert ist: `10`.
Maximale Wartezeit für eine Serverantwort (Sek.)	Die maximale Wartezeit auf eine Antwort vom NDR-Server in Sekunden. Der Standardwert ist: `10`.

Serverzertifikat	Die Einstellungsgruppe enthält Schaltflächen zum Hinzufügen und Entfernen eines Serverzertifikats:
	• **Hinzufügen** – Öffnet ein Fenster zum Hinzufügen eines Serverzertifikats. Die Schaltfläche wird angezeigt, wenn noch kein Serverzertifikat hinzugefügt wurde.
	Im Fenster zum Hinzufügen eines Zertifikats können Sie ein NDR-Serverzertifikat auf eine der folgenden Arten hinzufügen:
	  • Geben Sie im Feld **Aus Datei hinzufügen** den Pfad zu der Zertifikatsdatei an, die das Zertifikat im DER- oder PEM-Format enthält. Mit der Schaltfläche **Durchsuchen** wird ein Standardfenster für die Dateiauswahl geöffnet.
	  • Kopieren Sie den Inhalt der Zertifikatsdatei in das Feld **Zertifikatdaten einfügen**.
	Wenn ein Serverzertifikat hinzugefügt wurde, wird das Serverzertifikat auf Seiten von Kaspersky Endpoint Security überprüft. Dies erhöht die Sicherheit der Verbindung.
	• **Löschen** – Entfernt ein zuvor hinzugefügtes Serverzertifikat. Diese Schaltfläche wird angezeigt, wenn ein Serverzertifikat hinzugefügt wurde.

Erweiterter Schutz der Verbindung	Die Einstellungsgruppe enthält Oberflächenelemente, mit denen die Zwei-Wege-Authentifizierung konfiguriert wird. Diese dient einer zusätzlichen Absicherung der Verbindung:
	• **Zwei-Wege-Authentifizierung verwenden** – Aktiviert oder deaktiviert die Verwendung der Zwei-Wege-Authentifizierung für eine zusätzliche Absicherung der Verbindung zum NDR-Server. Um die bidirektionale Authentifizierung zu verwenden, müssen Sie ein Client-Zertifikat hinzufügen.
	  Auf der Seite des NDR-Servers muss die bidirektionale Authentifizierung aktiviert sein.
	• **Hinzufügen** – Öffnet ein Fenster zum Hinzufügen eines Client-Zertifikats, um die Verbindung mit dem NDR-Server zusätzlich abzusichern. Die Schaltfläche wird angezeigt, wenn das Kontrollkästchen **Zwei-Wege-Authentifizierung verwenden** aktiviert ist und noch kein Client-Zertifikat hinzugefügt wurde.
	Um ein Client-Zertifikat hinzuzufügen, geben Sie im Fenster zum Hinzufügen des Zertifikats den Pfad zu dem Krypto-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. Geben Sie anschließend das Kennwort für das Client-Zertifikat im Feld **Kennwort für Crypto-Container** ein.
	  Das Feld ist ein Pflichtfeld. Wenn Sie versuchen, die Einstellungen ohne Eingabe eines Kennworts zu speichern, wird eine Fehlermeldung angezeigt.
	Wenn das Kennwort korrekt ist, wird die Schaltfläche **OK** aktiv. Sie können die Einstellungen speichern.
	• **Löschen** – Entfernt ein zuvor hinzugefügtes Client-Zertifikat. Die Schaltfläche wird nur angezeigt, wenn ein Client-Zertifikat hinzugefügt wurde.

Datenübertragung an die NDR-Server konfigurieren

In diesem Fenster können Sie die Einstellungen für die Datenübertragung an die NDR-Server konfigurieren.

Einstellungen zur Datenübertragung an die NDR-Server

Parameter	Description
Maximale Verzögerung beim Versenden von Ereignissen (Sek.)	Maximale Verzögerung beim Senden von Ereignissen an den NDR-Server in Sekunden. Der Standardwert ist: `30`.
Maximale Anzahl an Ereignissen pro Paket	Die maximale Anzahl von Ereignissen in einem Paket. Der Standardwert ist: `1024`.
Häufigkeit der Serverabfragen	Häufigkeit des Sendens von Synchronisierungsanfragen an den NDR-Server in Sekunden. Der Standardwert ist: `450`.
Begrenzung für die Anzahl an Ereignissen aktivieren	Aktiviert oder deaktiviert die Beschränkung der Anzahl an Ereignissen, die an den NDR-Server gesendet werden.
Maximale Anzahl an Ereignissen pro Stunde	Maximale Anzahl an Ereignissen pro Stunde Der Standardwert ist: `3000`.
Prozentuale Überschreitung der Beschränkung der Ereignisanzahl	Prozentuale Überschreitung der Beschränkung der Ereignisanzahl: 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 KUMA

In der Verwaltungskonsole können Sie die Integration von Kaspersky Endpoint Security mit Kaspersky Unified Monitoring and Analysis Platform aktivieren oder deaktivieren und die Integrationseinstellungen in den Richtlinieneigenschaften verwalten (**KUMA-Integration** → **KUMA-Integration**).

Integrationseinstellungen für Kaspersky Unified Monitoring and Analysis Platform

Parameter	Description
Integration mit KUMA aktivieren	Aktiviert oder deaktiviert die Integration von Kaspersky Endpoint Security mit der Lösung Kaspersky Unified Monitoring and Analysis Platform. Die Integration mit KUMA ist standardmäßig deaktiviert.
Verschlüsselte Verbindung verwenden	Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung der Überprüfung des Serverzertifikats, um die Verbindung zum KUMA-Server zusätzlich abzusichern. Um das Serverzertifikat zu überprüfen, müssen Sie dieses Kontrollkästchen aktivieren und das Serverzertifikat im Fenster KUMA-Server hinzufügen. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
KUMA-Server	Wenn Sie auf die Schaltfläche **Konfigurieren** klicken, wird das Fenster KUMA-Server geöffnet. In diesem Fenster können Sie die Verbindungen zu den KUMA-Servern konfigurieren und die Liste der Server anzeigen, für welche eine Verbindung konfiguriert ist.
Einstellungen für die Verbindung mit dem KUMA-Server	Durch Klick auf die Schaltfläche **Konfigurieren** wird das Fenster Einstellungen für die Verbindung mit dem Server geöffnet. Dort können Sie die allgemeinen Einstellungen für die Verbindung mit den KUMA-Servern konfigurieren, ein Serverzertifikat hinzufügen und die Zwei-Wege-Authentifizierung für die Verbindung mit KUMA-Servern konfigurieren.
Maximale Verzögerung beim Versenden von Ereignissen (Sek.)	Maximale Verzögerung beim Senden von Ereignissen an den KUMA-Server in Sekunden. Der Standardwert ist: `30`.

Fenster "KUMA-Server" (mehrere)

Dieses Fenster zeigt in Tabellenform eine Liste mit Einstellungen für die Verbindung zu den KUMA-Servern an. Für jeden Server, zu dem eine Verbindung konfiguriert ist, enthält die Tabelle folgende Informationen:

- IP-Adresse (IPv4 oder IPv6) oder den vollständig qualifizierten Domänennamen (FQDN) des Servers. Wenn Sie im Fenster zur Konfiguration der KUMA-Integration das Kontrollkästchen **Verschlüsselte Verbindung verwenden** aktiviert haben, müssen Sie den vollständig qualifizierten Domänennamen (FQDN) des Servers aus dem Zertifikat angeben, das Sie beim Erwerb einer Lizenz zur Verwendung von KUMA erhalten haben.
- Port für die Verbindung zum KUMA-Server.
- Protokoll der Verbindung zum KUMA-Server.

Mit den Schaltflächen und dem Menü über der Tabelle können Sie Folgendes tun:

- Verbindungseinstellungen zu einem KUMA-Server hinzufügen.
- Bereits konfigurierte Verbindungseinstellungen ändern oder löschen.
- Eine Liste mit den konfigurierten Verbindungseinstellungen exportieren oder importieren.

Fenster "KUMA-Server"

In diesem Fenster können Sie die Parameter für die Verbindung zum KUMA-Server festlegen.

Einstellungen für die Verbindung mit den KUMA-Servern

Parameter	Description
Adresse	Die IP-Adresse (IPv4 oder IPv6) oder der vollqualifizierte Domänenname (FQDN) des KUMA-Integrationsservers kann angegeben werden. Wenn Sie im Fenster zur Konfiguration der KUMA-Integration das Kontrollkästchen **Verschlüsselte Verbindung verwenden** aktiviert haben, müssen Sie den vollständig qualifizierten Domänennamen (FQDN) des Servers aus dem Zertifikat angeben, das Sie beim Erwerb einer Lizenz zur Verwendung von KUMA erhalten haben.
Port	Port für die Verbindung zum KUMA-Server. Der Standardwert ist: `443`.
Protokoll	Protokoll für die Verbindung mit dem KUMA-Server: TCP, UDP oder HTTP/HTTPS mit Komprimierung. Wenn Sie das UDP-Protokoll auswählen, wird die Verwendung von Zertifikaten für eine sichere Verbindung nicht unterstützt und es werden keine Ereignisse über die Verbindung mit dem KUMA-Server generiert. Standardwert: TCP.

Fenster "Einstellungen für die Verbindung mit den KUMA-Servern"

In diesem Fenster können Sie die allgemeinen Verbindungseinstellungen mit den KUMA-Servern konfigurieren.

Einstellungen für die Verbindung mit den KUMA-Servern

Parameter	Description
Maximale Wartezeit für die Verbindung zum Server (Sek.)	Die maximale Wartezeit auf eine Verbindung mit dem KUMA-Server in Sekunden. Der Standardwert ist: `5`.
Serverzertifikat	Die Einstellungsgruppe enthält Schaltflächen zum Hinzufügen und Entfernen eines Serverzertifikats.

Parameter	Description
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.
Erweiterter Schutz der Verbindung	Die Einstellungsgruppe enthält Oberflächenelemente, mit denen die Zwei-Wege-Authentifizierung konfiguriert wird. Diese dient einer zusätzlichen Absicherung der Verbindung.
Zwei-Wege-Authentifizierung verwenden	Das Kontrollkästche aktiviert oder deaktiviert die Verwendung der Zwei-Wege-Authentifizierung für eine zusätzliche Absicherung der Verbindung zum KUMA-Server. Um die bidirektionale Authentifizierung zu verwenden, müssen Sie ein Client-Zertifikat hinzufügen. Auf der Seite des KUMA-Servers muss die bidirektionale Authentifizierung aktiviert sein.
Hinzufügen (des Client-Zertifikats)	Öffnet ein Fenster zum Hinzufügen eines Client-Zertifikats, um die Verbindung mit dem KUMA-Server abzusichern. Die Schaltfläche wird angezeigt, wenn noch kein Client-Zertifikat hinzugefügt wurde. Wenn Sie die Verbindung zusätzlich absichern möchten, müssen Sie der Seite des KUMA-Servers die Überprüfung von Client-Zertifikaten 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.

Fenster zum Hinzufügen eines Serverzertifikats

In diesem Fenster können Sie das Zertifikat eines KUMA-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 eingeben** kopieren.

Wenn ein Serverzertifikat hinzugefügt wurde, wird das Serverzertifikat auf Seiten von Kaspersky Endpoint Security überprüft. Dies erhöht die Sicherheit der Verbindung.

Fenster zum Hinzufügen eines Client-Zertifikats

In diesem Fenster können Sie ein Client-Zertifikat hinzufügen, um die Verbindung mit dem KUMA-Server zusätzlich abzusichern.

Wenn Sie die Verbindung zusätzlich absichern möchten, müssen Sie auf der Seite des KUMA-Servers die Überprüfung von Client-Zertifikaten aktivieren und das Kontrollkästchen **Zwei-Wege-Authentifizierung** im Fenster **Einstellungen für die Verbindung mit den KUMA-Servern** aktivieren.

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. Geben Sie anschließend das Kennwort für das Client-Zertifikat im Feld **Kennwort für Crypto-Container** ein.

Das Feld ist ein Pflichtfeld. Wenn Sie versuchen, die Einstellungen ohne Eingabe eines Kennworts zu speichern, wird eine Fehlermeldung angezeigt.

Wenn das Kennwort korrekt ist, wird die Schaltfläche **OK** aktiv. Sie können die Einstellungen speichern.

Quarantäne

In der Verwaltungskonsole können Sie Quarantäne-Einstellungen in den Eigenschaften der Richtlinie (**Allgemeine Einstellungen** → **Speichereinstellungen**) und in den Eigenschaften verwalteter Geräte (**Verwaltete Geräte** → Registerkarte **Geräte** → Fenster mit den Geräteeigenschaften → Abschnitt **Anwendungen** → Fenster mit den App-Eigenschaften → **Speichereinstellungen**) verwalten.

Quarantäne-Einstellungen

Parameter	Description
Größe der Quarantäne begrenzen auf (MB)	Das Kontrollkästchen aktiviert oder deaktiviert die Begrenzung der maximalen Größe des Quarantäne-Speichers auf einen angegebenen Wert (in Megabyte). Wenn kein Häkchen gesetzt wurde, ist die Größe der Quarantäne unbegrenzt. Zulässige Werte: 1 – 999999. Der Standardwert ist 200, wenn die App im Standard-Modus oder im EDR Agent-Modus verwendet wird, und 100, wenn die App im Light Agent-Modus verwendet wird.
Benachrichtigen, wenn Quarantäne gefüllt ist zu (%)	Das Kontrollkästchen aktiviert oder deaktiviert die prozentuale Begrenzung des Füllstandes der Quarantäne, bei dessen Erreichen ein Ereignis über den Füllstand der Quarantäne generiert wird. Wenn das Kontrollkästchen deaktiviert ist, werden keine Ereignisse zum Quarantäne-Füllstand generiert. Zulässige Werte: 1 – 100. Standardwert: 90.

Ausführungsprävention für Objekte

Sie können die Ausführungsprävention für Objekte in der Verwaltungskonsole nur aktivieren oder deaktivieren, wenn die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA) aktiviert ist.

Sie können die Ausführungsprävention für Objekte in den Richtlinieneigenschaften aktivieren oder deaktivieren (**Programmeinstellungen** → **Detection and Response** → **EDR Expert (on-premise)**).

Das Kontrollkästchen **Ausführungsprävention für Objekte aktivieren** unter **Ausführungsprävention für Objekte** aktiviert bzw. deaktiviert die Regeln von EDR Expert (on-premise) für die Ausführungsprävention für Objekte.

Allgemeine Einstellungen

In der Verwaltungskonsole können Sie in den Eigenschaften der Richtlinie (**Allgemeine Einstellungen**) allgemeine Programmeinstellungen verwalten, die den Betrieb des Programms insgesamt sowie den Betrieb einzelner Funktionen festlegen.

Proxy-Server

In der Verwaltungskonsole können Sie die Proxyserver-Einstellungen in den Richtlinieneigenschaften verwalten (**Allgemeine Einstellungen → Proxyserver-Einstellungen**).

Proxy-Server-Einstellungen

Parameter	Description
Keinen Proxyserver verwenden	Wenn diese Option ausgewählt ist, wird der Proxyserver bei der Ausführung der Anwendung nicht verwendet.
Angegebene Proxyserver-Einstellungen verwenden	Wenn diese Option ausgewählt ist, verwendet Kaspersky Endpoint Security die angegebenen Proxyserver-Parameter für die folgenden Vorgänge: für den Zugriff auf die Aktivierungsserver von Kaspersky, auf die Update-Quellen für Datenbanken und Module der Anwendung und auf Kaspersky Security Network sowie für die Untersuchung von Website-Zertifikaten mit dem Schutz vor Web-Bedrohungen.
Adresse und Port	Felder zur Eingabe der IP-Adresse bzw. des Domänennamens und des Ports des Proxyservers. Standardwert: 3128. Die Felder sind verfügbar, wenn die Option **Angegebene Proxyserver-Einstellungen verwenden** ausgewählt ist.
Authentifizierung am Proxyserver verwenden	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Authentifizierung mithilfe von Benutzername und Kennwort beim Zugriff auf den Proxyserver. Das Kontrollkästchen ist verfügbar, wenn die Variante **Angegebene Proxyserver-Einstellungen 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 verwendet eine unsichere Verbindung und das Benutzerkonto ist möglicherweise kompromittiert.
Benutzername	Eingabefeld für den Benutzernamen zur Authentifizierung des Benutzers auf dem Proxyserver. Das Eingabefeld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver 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 Proxyserver verwenden** aktiviert ist.
Kaspersky Security Center als Proxyserver für die Aktivierung der Anwendung verwenden	Aktiviert oder deaktiviert die Verwendung des Kaspersky Security Center Administrationsservers als Proxyserver für den Zugriff auf die Aktivierungsserver von Kaspersky. Dies ist erforderlich, wenn die Anwendung in einem isolierten Netzwerksegment ohne Internetzugang anhand eines Aktivierungscodes aktiviert wird. Wenn das Kontrollkästchen aktiviert ist, erhält die Anwendung über den Administrationsserver mit Internetzugang Zugriff auf die Aktivierungsserver. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Die Einstellung wird nur angewendet, wenn die Anwendung im Standard-Modus verwendet wird. Wenn das Programm im Light Agent-Modus verwendet wird, stellt der Schutzserver die Lizenzinformation bereit.
Proxyserver-Ausnahmen	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster Proxyserver-Ausnahmen öffnet.

Fenster "Proxyserver-Ausnahmen"

Dieses Fenster dient sowohl zur Konfiguration der Proxyserver-Verwendung bei einer Integration mit den Komponenten von Kaspersky Anti Targeted Attack Platform als auch zur Erstellung einer Liste von Adressen, für deren Verbindung der Proxyserver nicht verwendet wird.

Proxyserver-Ausnahmen

Parameter	Description
Für diese Komponenten keinen Proxyserver verwenden	Aktivieren Sie die Kontrollkästchen neben den Programmkomponenten, für die der Proxyserver nicht verwendet werden soll: • **Endpoint Detection and Response Expert (on-premise)** – beim Herstellen einer Verbindung mit Servern, die die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA) bereitstellen, keinen Proxyserver verwenden. • **Sandbox** – Keinen Proxyserver für die Verbindung mit Servern verwenden, welche die Integration mit Sandbox gewährleisten. • **Network Detection and Response (KATA)** – Keinen Proxyserver für die Verbindung mit Servern verwenden, welche die Integration mit Kaspersky Network Detection and Response (KATA) gewährleisten.
Für diese Adressen keinen Proxyserver verwenden	Die Tabelle enthält Liste von Adressen, für deren Verbindung kein Proxyserver verwendet wird: • **IP-Adresse/DNS-Name** – für die Verbindung mit der IP-Adresse oder dem DNS-Namen wird kein Proxyserver verwendet. Für die Angabe der Adressen können Masken verwendet werden (Symbole `*` und `?`). • **Kommentar** – Eingabefeld für einen Kommentar (optional). In der Tabelle können Sie Adressen hinzufügen, bearbeiten oder löschen.

CPU-Auslastung durch Untersuchungsaufgaben

In der Verwaltungskonsole können Sie die Begrenzung der CPU-Auslastung aktivieren oder deaktivieren und die Begrenzung der Speichernutzung für Untersuchungsaufgaben in den Richtlinieneigenschaften konfigurieren (**Allgemeine Einstellungen** → **App-Einstellungen**, Abschnitt **Leistung**).

Durch Klicken auf **Konfigurieren** unter **Leistung** wird das Fenster **Leistungseinstellungen für Untersuchungsaufgaben** geöffnet, in dem Sie im Abschnitt **Prozessor- und Speicherauslastung** Grenzwerte konfigurieren können (siehe Tabelle unten).

Einstellungen für CPU- und Speicherauslastung

Parameter	Description
Prozessorauslastung 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 rechts (in Prozent) nicht überschreiten. Der Wert im Feld muss eine Ganzzahl zwischen 10 und 100 sein. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Begrenzung der Speichernutzung für Untersuchungsaufgaben (MB)	Eingabefeld zur Begrenzung für die Speichernutzung der Untersuchungsaufgaben (in MB). Standardwert: 8192.

Ausführen von Aufgaben im Akkubetrieb

In der Verwaltungskonsole können Sie das Abbrechen geplanter Aufgaben in den Richtlinieneigenschaften konfigurieren (**Allgemeine Einstellungen** → **App-Einstellungen**, Abschnitt **Leistung**).

Aufgabeneinstellungen im Akkubetrieb

Parameter	Description
Geplante Aufgaben im Akkubetrieb überspringen	Dieses Kontrollkästchen aktiviert oder deaktiviert den Abbruch geplanter Aufgaben. Dieses Kontrollkästchen ist standardmäßig aktiviert. Bei deaktiviertem Kontrollkästchen werden alle geplanten Aufgaben auf dem Gerät ausgeführt, unabhängig von der Stromquelle, die das Gerät nutzt (Netz oder Batterie).

App starten

In der Verwaltungskonsole können Sie die Starteinstellungen der App in den Richtlinieneigenschaften verwalten (**Allgemeine Einstellungen** → **App-Einstellungen**, Abschnitt **Starteinstellungen der App**).

Wenn Sie im Block **Starteinstellungen der Anwendung** auf die Schaltfläche **Konfigurieren** klicken, wird das Fenster **Starteinstellungen der Anwendung** geöffnet, in dem Sie die Einstellungen für den Start der Anwendung konfigurieren können (siehe Tabelle unten).

Starteinstellungen der Anwendung

Parameter	Description
Maximale Anzahl an fehlgeschlagenen Versuchen, die Anwendung zu starten	Maximale Anzahl an fehlgeschlagenen Versuchen, die Anwendung zu starten. Standardwert: 5.
Maximale Wartezeit für den Anwendungsstart (Min.)	Eingabefeld für die maximale Wartezeit auf den Start der Anwendung (in Minuten), nach deren Überschreitung der Prozess "kesl" neu gestartet wird. Standardwert: 3.

Automatischer Neustart, wenn ein kritisches Update empfangen wird

In der Verwaltungskonsole können Sie den automatischen Neustart des Programms bei der Installation kritischer Updates in den Richtlinieneigenschaften konfigurieren (**Allgemeine Einstellungen** → **App-Einstellungen**).

Wenn Sie im Abschnitt **Erweiterte App-Einstellungen** auf die Schaltfläche **Konfiguration** klicken, wird das Fenster **Zusätzliche Einstellungen** geöffnet, in dem Sie den Neustart des Programms beim Erhalt kritischer Updates konfigurieren können (siehe Tabelle unten).

Einstellungen für die Anwendung kritischer Updates

Parameter	Description
Programm beim Erhalt kritischer Updates automatisch neu starten	Mit diesem Kontrollkästchen wird der automatische Neustart des Programms aktiviert bzw. deaktiviert, wenn kritische Updates nach Ablauf der ersten 24 Stunden nach der Programminstallation empfangen werden. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Wenn dieses Kontrollkästchen aktiviert ist, wird das Programm nach dem Erhalt kritischer Updates neu gestartet, wenn seit der Installation 24 Stunden vergangen sind.

Kennwortschutz

In der Verwaltungskonsole können Sie die Einstellungen für den Kennwortschutz in den Richtlinieneigenschaften konfigurieren (**Allgemeine Einstellungen** → **Benutzeroberfläche**, im Abschnitt **Kennwortschutz**).

Unter **Kennwortschutz** öffnet ein Klick auf die Schaltfläche **Konfigurieren** das Fenster **Einstellungen des Kennwortschutzes**, in dem Sie die Einstellungen für den Kennwortschutz bearbeiten können (siehe Tabelle unten).

Starteinstellungen der Anwendung

Parameter	Description
Kennwortschutz aktivieren	Dieses Kontrollkästchen aktiviert oder deaktiviert den Kennwortschutz für Programmeinstellungen. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Berechtigungen	Diese Tabelle enthält Benutzer und Gruppen, für die Sie Berechtigungen zum Ändern der Programmeinstellungen konfigurieren können. Die Tabelle umfasst die folgenden Spalten: • **Benutzer/Gruppe** ist der Name des lokalen Benutzers oder Domänenbenutzers oder der Name der Benutzergruppe, für die Berechtigungen konfiguriert sind. • **Typ** ist entweder **Benutzer** oder **Gruppe**, wofür Berechtigungen konfiguriert sind. • **Berechtigungen** ist eine Liste der Vorgänge, die der Benutzer oder die Gruppe ausführen darf. Sie können Benutzergruppen hinzufügen, anpassen und löschen. Sie können auf die Schaltfläche **Hinzufügen** klicken, um das Fenster **Berechtigungen für Benutzer bzw. Gruppe** zu öffnen, in dem Sie einen Benutzer oder eine Gruppe hinzufügen und Berechtigungen zum Ändern der Programmeinstellungen festlegen können.

Trace- und Dump-Einstellungen

In der Verwaltungskonsole können Sie die Trace- und Dump-Einstellungen in den Eigenschaften der Richtlinie verwalten (**Allgemeine Einstellungen** → **Programmeinstellungen**, Abschnitt **Trace- und Dump-Einstellungen**).

Wenn Sie unter **Trace- und Dump-Einstellungen** auf **Konfigurieren** klicken, wird das Fenster **Trace- und Dump-Einstellungen** geöffnet, in dem Sie die Einstellungen für Trace- und Dump-Dateien bearbeiten können (siehe Tabelle unten).

Trace- und Dump-Einstellungen

Parameter	Description
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 der Benutzer, der Kaspersky Endpoint Security ausführt, Lese- und Schreibberechtigungen für dieses Verzeichnis besitzt. Für den Zugriff auf das Standardverzeichnis mit Protokolldateien sind Root-Rechte erforderlich.
Maximale Größe der Protokolldatei (MB)	In diesem Feld können Sie die maximale Größe einer Ablaufverfolgungsdatei für das Programm eingeben (in Megabyte). Standardwert: 500.
Maximale Anzahl der Protokolldateien	In diesem Feld können Sie die maximale Anzahl von Ablaufverfolgungsdateien für das Programm eingeben. Standardwert: 10.
Bei Absturz der Anwendung eine Dump-Datei erstellen	Das Kontrollkästchen aktiviert oder deaktiviert die Erstellung einer Dump-Datei, wenn die Anwendung 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.

Von der Anwendung genutzter residenter Speicher

In der Verwaltungskonsole können Sie die Beschränkung für die Nutzung des residenten Speichers in den Richtlinieneigenschaften konfigurieren (**Allgemeine Einstellungen** → **App-Einstellungen**).

Wenn Sie im Block **Erweiterte Einstellungen der Anwendung** 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).

Um die Änderungen zu übernehmen, starten Sie Kaspersky Endpoint Security auf dem verwalteten Gerät neu, nachdem die Richtlinie übernommen wurde.

Einstellungen für die Nutzung des residenten Speichers durch die Anwendung

Einstellung	Description
Speichernutzung der Anwendung	In der Dropdown-Liste können Sie auswählen, auf welche Weise die Verwendung des residenten Speichers begrenzt werden soll: • **Nicht begrenzen**. 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 **Begrenzung des genutzten Speichers (%)** verfügbar, in dem Sie den gewünschten Prozentwert angeben können. • **Grenzwert in Megabyte**. Wenn diese Option ausgewählt ist, wird das Feld **Begrenzung des genutzten Speichers (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 **Begrenzung des genutzten Speichers (%)** und **Begrenzung des genutzten Speichers (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 **Begrenzung des genutzten Speichers (%)** und **Begrenzung des genutzten Speichers (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.

Untersuchung verschlüsselter Verbindungen

In der Verwaltungskonsole können Sie die Einstellungen für die Untersuchung des Netzwerkverkehrs in den Richtlinieneigenschaften verwalten (**Allgemeine Einstellungen** → **Netzwerkeinstellungen**).

Parameter	Description
Untersuchung verschlüsselter Verbindungen aktivieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von verschlüsselten Verbindungen. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Parameter für verschlüsselte Verbindungen	Der Block enthält die Einstellungen zur Untersuchung verschlüsselter Verbindungen:
	• **Besuch einer Domäne mit nicht vertrauenswürdigem Zertifikat** gibt die Aktion an, die die App ausführen muss, wenn eine Domäne mit nicht vertrauenswürdigem Zertifikat besucht wird:
	  • **Erlauben** (Standardwert) – Verbindung zu einer Domäne mit einem nicht vertrauenswürdigen Zertifikat zulassen.
	  • **Blockieren** – Verbindung zu einer Domäne mit einem nicht vertrauenswürdigen Zertifikat blockieren.
	• **Zu Domäne mit Fehler bei der Untersuchung des Netzwerkverkehrs wechseln** – Aktion, die von der Anwendung beim Übergang zu einer Domäne mit einem Fehler bei der Untersuchung des Netzwerkverkehrs ausgeführt wird:
	  • **Domäne zu den Ausnahmen 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** – Methode, mit der die Anwendung Zertifikate überprüft:
	  • **Lokale Überprüfung**: Die App überprüft ein Zertifikat, ohne das Internet zu verwenden.
	  • **Vollständige Überprüfung** (Standardwert) – Die Anwendung 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	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Vertrauenswürdige Stammzertifikate** geöffnet. In diesem Fenster können Sie eine Liste von Stammzertifikaten konfigurieren, die Kaspersky Endpoint Security bei der Untersuchung verschlüsselter Verbindungen als vertrauenswürdig einstuft.
Ausnahmen vom Abfangen des Datenverkehrs	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Ausnahmen vom Abfangen des Datenverkehrs** öffnet. In diesem Fenster können Sie die Parameter für Verbindungen konfigurieren, deren Datenverkehr die Anwendung vom Abfangen ausschließt.
Einstellungen der Netzwerkports	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Überwachte Ports** geöffnet.
Erweiterte Einstellungen	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Modus für das Abfangen des Datenverkehrs** öffnet. In diesem Fenster können Sie den von der Anwendung verwendeten Modus zum Abfangen des Datenverkehrs konfigurieren: • **eBPF-Technologie verwenden**. Wenn diese Option ausgewählt ist, verwendet die Anwendung die eBPF-Technologie zum Abfangen des Datenverkehrs. • **iptables-Tool verwenden** (Standardwert). Wenn diese Option ausgewählt ist, verwendet die Anwendung iptables-Tool zum Abfangen des Datenverkehrs. Um den Modus zum Abfangen des Datenverkehrs zu ändern, muss die Anwendung neu gestartet werden. Während des Neustarts werden bestehende Netzwerkverbindungen unterbrochen.

Fenster "Vertrauenswürdige Domänen"

Diese Liste enthält Domänennamen und Masken für Domänennamen, die von der Untersuchung ausgenommen werden. Die Anwendung untersucht keine Verbindungen, die beim Aufruf bestimmter Domänen hergestellt wurden.

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.

Fenster "Vertrauenswürdige Zertifikate"

Sie können eine Liste mit Stammzertifikaten konfigurieren, die von Kaspersky Endpoint Security als vertrauenswürdig eingestuft werden. Die Liste der vertrauenswürdigen Stammzertifikate wird bei der Untersuchung verschlüsselter Verbindungen verwendet.

Für jedes Zertifikat werden folgende Daten angezeigt:

- Zertifikatinhaber
- Seriennummer des Zertifikats
- 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.

Durch Klicken auf die Schaltfläche **Hinzufügen** öffnet sich ein Fenster, in dem Sie ein Zertifikat auf eine der folgenden Arten zur Liste der vertrauenswürdigen Zertifikate hinzufügen können:

- 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 eingeben** kopieren.

Fenster "Ausnahmen vom Abfangen des Datenverkehrs"

Die Tabelle enthält die Parameter der Verbindung, welche die Anwendung vom Abfangen des Datenverkehrs ausschließt:

- **Remote-IP-Adresse** – Datenverkehr von oder zu dieser Adresse (je nach Richtung des Datenverkehrs) wird vom Abfangen ausgeschlossen.
- **Zielport** – Port auf dem geschützten Gerät (wenn eingehender Datenverkehr vom Abfangen ausgeschlossen wird) oder Port auf dem Remote-Gerät (wenn ausgehender Datenverkehr vom Abfangen ausgeschlossen wird).
- **Richtung des Datenverkehrs** – Richtung des Datenverkehrs der Verbindung: eingehend oder ausgehend.

Sie können Ausnahmen hinzufügen, bearbeiten und löschen.

Fenster "Ausnahme vom Abfangen des Datenverkehrs"

In diesem Fenster können Sie dem Abfangen des Datenverkehrs eine Ausnahme hinzufügen. Dazu müssen Sie die folgenden Verbindungsparameter angeben:

- **Remote-IP-Adresse** – Adresse des Remote-Geräts im IPv4- oder IPv6-Format. Je nach Richtung des Datenverkehrs wird der Datenverkehr entweder von der angegebenen IP-Adresse (Ausschließen des eingehenden Datenverkehrs) oder zu der angegebenen IP-Adresse (Ausschließen des ausgehenden Datenverkehrs) ausgeschlossen.

- **Zielport** – je nach Richtung des Datenverkehrs:

  - Port auf dem geschützten Gerät (Ausschließen des eingehenden Datenverkehrs). Der Datenverkehr vom Remote-Gerät zu diesem Port wird vom Abfangen ausgeschlossen.

  - Port auf dem Remote-Gerät (Ausschließen des ausgehenden Datenverkehrs). Der Datenverkehr vom geschützten Gerät zu diesem Port wird vom Abfangen ausgeschlossen.

- **Richtung des Datenverkehrs** – Richtung des Datenverkehrs der ausgeschlossenen Verbindung. Sie können eine Ausnahme für eingehenden oder ausgehenden Datenverkehr einrichten.

Sie können in der Ausnahme entweder nur die IP-Adresse eines Remote-Geräts oder den Zielport angeben.

Wenn Sie für eine eingehende Ausnahme nur die IP-Adresse eines Remote-Geräts angeben (ohne Port des geschützten Geräts), wird der gesamte Datenverkehr vom Remote-Gerät vom Abfangen ausgeschlossen. Es wird empfohlen, eine solche Ausnahme nur für Datenverkehr von Geräten einzurichten, denen Sie vertrauen.

Fenster "Überwachte Ports"

Einstellungen der Netzwerkports

Parameter	Description
Alle Netzwerkports überwachen	Wenn diese Aktion ausgewählt ist, überwacht die App alle Netzwerkports.
Nur ausgewählte Netzwerkports überwachen	Wenn diese Aktion ausgewählt ist, überwacht die Anwendung nur die in der Tabelle angegebenen Netzwerkports. Diese Option ist standardmäßig ausgewählt.
Einstellungen der Netzwerkports	Die Tabelle enthält die Netzwerkports, die von der Anwendung untersucht werden, wenn die Aktion **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.

Globale Ausnahmen

In der Verwaltungskonsole können Sie globale Ausnahmen in den Richtlinieneigenschaften konfigurieren (**Allgemeine Einstellungen** → **Globale Ausnahmen**).

Die Einstellungsgruppe **Ausgenommene Einhängepunkte** enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Ausgenommene Einhängepunkte** geöffnet.

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.

Fenster "Pfad zum Mountpunkt"

Einstellungen des Mountpunkts

Parameter	Description
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 Masken verwendet werden. Die Mountpunkte müssen genau so angegeben werden, wie sie in der Ausgabe des Befehls `mount` angezeigt werden.
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.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Ausschließen des Prozessspeichers von Untersuchungen

In der Verwaltungskonsole können Sie in den Richtlinieneigenschaften (**Allgemeine Einstellungen** → **Prozessspeicher ausschließen**) das Ausschließen des Prozessspeichers von Untersuchungen konfigurieren.

Durch Klicken auf die Schaltfläche **Konfigurieren** im Block **Prozess-Speicher von der 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, welche die Anwendung von der Untersuchung des Prozess-Speichers ausschließt. Bei der Angabe des Pfades können Masken verwendet werden. Standardmäßig ist die Liste leer.

Sie können die Vereinigung der Ausschlusslisten aktivieren, wenn diese von untergeordneten Richtlinien geerbt werden. Um die Listenelemente zu vereinen, müssen Sie im Fenster **Prozess-Speicher von der Untersuchung ausschließen** das Kontrollkästchen **Werte bei Vererbung vereinen** aktivieren. Wenn das Kontrollkästchen aktiviert ist, werden die Elemente der übergeordneten Richtlinienliste in den untergeordneten Richtlinien angezeigt und die Elemente können der untergeordneten Richtlinienliste hinzugefügt werden. Bei deaktiviertem Kontrollkästchen werden die Listenelemente beim Vererben von Richtlinieneinstellungen nicht vereinigt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Nützliche Artikel

So geben Sie Masken an

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. Beispielsweise `/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. Beispielsweise `/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.

Datenverwaltung

In der Verwaltungskonsole können Sie Backup-Einstellungen in den Richtlinieneigenschaften (**Allgemeine Einstellungen** → **Speichereinstellungen**) und in den Eigenschaften verwalteter Geräte (**Verwaltete Geräte** → Registerkarte **Geräte** → Fenster mit den Geräteeigenschaften → Abschnitt **Programme** → Fenster mit den Programmeigenschaften → **Speichereinstellungen**) verwalten.

Backup-Einstellungen

Parameter	Description
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 – 10000. Ist der Wert 0 angegeben, dann ist der Zeitraum der Speicherung der Objekte im Backup nicht begrenzt. Standardwert: 30.
Größe des Backup-Speichers begrenzen auf (MB)	Dieses Kontrollkästchen aktiviert oder deaktiviert die Begrenzung der maximalen Backup-Größe auf einen angegebenen Wert (in Megabyte). Zulässige Werte: 1 – 4000. Wenn kein Häkchen gesetzt wurde, ist die Größe des Backup-Speichers unbegrenzt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Erkennen von Anwendungen, die von Angreifern für Kompromittierungen ausgenutzt werden können

In der Verwaltungskonsole können Sie die Erkennung legitimer Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können, in den Eigenschaften der Richtlinie (**Allgemeine Einstellungen** → **App-Einstellungen**, Abschnitt **Untersuchungseinstellungen**) konfigurieren.

Einstellungen für die Erkennung von Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können

Parameter	Description
Legale Programme erkennen, die von Angreifern zur Beschädigung von Geräten oder Daten ausgenutzt werden können	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Erkennung legitimer Anwendungen, die von Angreifern zur Schädigung von Computern oder Benutzerdaten verwendet werden könnten. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Überwachung von Dateioperationen

In der Verwaltungskonsole können Sie den Modus zum Abfangen von Dateioperationen in den Richtlinieneigenschaften konfigurieren (**Allgemeine Einstellungen** → **App-Einstellungen**, Abschnitt **Modus zum Abfangen von Dateioperationen**).

Einstellungen zum Abfangen von Dateioperationen

Parameter	Description
Zugriff auf den Dateien während der Untersuchung blockieren	Dieses Kontrollkästchen aktiviert oder deaktiviert das Blockieren des Zugriffs auf Dateien, während diese durch die Komponenten Schutz vor bedrohlichen Dateien und Gerätekontrolle, die Aktion Ausführungsprävention und die Aufgabe Untersuchung von Wechseldatenträgern untersucht werden. Dieses 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.

Senden von Informationen an den Speicher von Kaspersky Security Center

In Kaspersky Security Center können Sie die Übertragung von Informationen über Dateien im Backup, Dateien in der Quarantäne, nicht verarbeitete Dateien und verbundene Geräte an den Speicher von Kaspersky Security Center aktivieren und deaktivieren.

Eine allgemeine Liste der Dateien, die von Kaspersky-Programmen auf Client-Geräten unter Quarantäne gestellt wurden, wird in Kaspersky Security Center gespeichert und ist auch in der Verwaltungskonsole (**Erweitert** → **Speicher** → **Quarantäne**) verfügbar.

Eine allgemeine Liste der Dateien, die von Kaspersky-Programmen auf Client-Geräten im Backup abgelegt wurden, wird in Kaspersky Security Center erstellt und ist in der Verwaltungskonsole (**Erweitert** → **Speicher** → **Backup**) verfügbar.

Informationen zu nicht verarbeiteten Dateien werden in der Liste der aktiven Bedrohungen 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 Hardwareliste in der Verwaltungskonsole (**Erweitert** → **Speicher** → **Hardware**) angezeigt. Informationen werden übertragen, wenn die Komponente Gerätekontrolle aktiviert ist.

Informationen zu Programmen, die auf dem Client-Gerät gefunden wurden, werden außerdem in der Liste der Programme in der Verwaltungskonsole (**Erweitert** → **Programmverwaltung** → **Programm-Registry**) angezeigt. Die Informationen werden übertragen, wenn die Komponente Programmkontrolle aktiviert ist.

Datenübertragung in der Verwaltungskonsole aktivieren und deaktivieren

In der Verwaltungskonsole können Sie die Datenübertragung an den Administrationsserver in den Richtlinieneigenschaften (**Allgemeine Einstellungen** → **Speichereinstellungen**, **Daten an den Administrationsserver übertragen**) oder in den Eigenschaften des verwalteten Geräts (**Verwaltete Geräte** → Registerkarte **Geräte** → Fenster mit den Geräteeigenschaften → Abschnitt **Programme** → Fenster mit den Programmeigenschaften → **Speichereinstellungen**, Abschnitt **Daten an den Administrationsserver übertragen**) aktivieren oder deaktivieren.

Durch Klick auf die Schaltfläche **Konfigurieren** im Block **Daten an den Administrationsserver übertragen** wird das Fenster **Einstellungen für die Datenübertragung** geöffnet. Dort können Sie das Senden von Informationen an den Administrationsserver aktivieren oder deaktivieren.

Parameter für die Übertragung von Daten zum Administrationsserver

Parameter	Description
Dateien in der Quarantäne	Das Kontrollkästchen aktiviert oder deaktiviert die Übertragung von Informationen über unter Quarantäne gestellte Dateien an den Administrationsserver. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Dateien im Backup	Das Kontrollkästchen aktiviert oder deaktiviert die Übertragung von Informationen über Dateien im Backup an den Administrationsserver. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Nicht verarbeitete Dateien	Dieses Kontrollkästchen aktiviert und deaktiviert das Senden von Benachrichtigungen über Dateien, die während der Untersuchung nicht verarbeiteten wurden, an den Administrationsserver. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Angeschlossene Geräte	Dieses Kontrollkästchen aktiviert oder deaktiviert die Übertragung von Informationen über die auf dem verwalteten Client-Gerät installierten Geräte an den Administrationsserver. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Anwendungen, die auf dem Gerät gefunden wurden	Das Kontrollkästchen aktiviert oder deaktiviert die Übertragung der Liste mit den Anwendungen, die durch die Inventarisierungsaufgabe auf dem Client-Gerät erkannt wurden, an den Administrationsserver. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Abfangen von Systemereignissen

In der Verwaltungskonsole können Sie das Abfangen von Systemereignissen in den Richtlinieneigenschaften konfigurieren (**Allgemeine Einstellungen → Einstellungen für die Interaktion mit dem Betriebssystem**, Abschnitt **Einstellungen für das Abfangen von Systemereignissen**).

Die Parameter werden nur auf Geräten angewendet, deren Betriebssystem die fanotify-Technologie unterstützt.

Abfangen von Systemereignissen

Parameter	Description
Abfangmechanismus	Der von der Anwendung verwendete Mechanismus zum Abfangen von Systemereignissen: • **fanotify-Technologie** (Standardwert). Wenn diese Option ausgewählt ist, verwendet das Programm die Fanotify-Technologie zum Abfangen von Systemereignissen. • **Aktualisierbares Kernel-Modul**. Wenn diese Option ausgewählt ist, verwendet das Programm das aktualisierbare Kernel-Modul zum Abfangen von Systemereignissen.
Wenn aktualisierbares Kernel-Modul nicht ausführbar	Aktion, die das Programm ausführt, wenn das aktualisierbare Kernel-Modul nicht gestartet werden kann: • **fanotify-Technologie verwenden** (Standardwert). Wenn diese Option ausgewählt ist, wechselt das Programm zur Fanotify-Technologie zum Abfangen von Systemereignissen. • **Abfangen von Systemereignissen deaktivieren** Wenn die App das Abfangen von Systemereignissen nicht verwendet, wird keine Echtzeituntersuchung von Dateien ausgeführt und die Schutzstufe des Geräts sinkt. Dieser Parameter ist verfügbar, wenn als Abfangmechanismus die Option **Aktualisierbares Kernel-Modul** ausgewählt ist.

Erweiterte Einstellungen zur Erfassung von Telemetriedaten

In der Verwaltungskonsole können Sie zusätzliche Einstellungen für Telemetriedaten in den Richtlinieneigenschaften verwalten (**Allgemeine Einstellungen → Einstellungen für die Interaktion mit dem Betriebssystem**, Abschnitt **Zusätzliche Einstellungen für Telemetriedaten**).

Erweiterte Einstellungen zur Erfassung von Telemetriedaten

Parameter	Description
Quelle der Telemetriedaten	Die Quelle, die Kaspersky Endpoint Security zur Erfassung von Telemetriedaten verwendet: • **Nur eBPF verwenden** – Zur Erfassung von Telemetriedaten wird ausschließlich die eBPF-Technologie verwendet. • **eBPF und auditd verwenden** (Standardwert) – Zur Erfassung von Telemetriedaten wird die eBPF-Technologie und der auditd-Dienst verwendet.
Verwendung von auditd	Nutzungsmodus des auditd-Dienstes: • **Im exklusiven Modus** (Standardwert) – Die Anwendung "Kaspersky Endpoint Security" verwendet den Dienst "auditd" im exklusiven Modus. • **Im Multicast-Modus** – Der Dienst "auditd" wird im Multicast-Modus verwendet. Diese Einstellung wird nur angewendet, wenn für den Parameter **Quelle der Telemetriedaten** die Variante **eBPF und auditd verwenden** ausgewählt ist.

Light Agent-Modus

In der Verwaltungskonsole können Sie die Einstellungen für die Verbindung des Light Agents mit SVMs in den Richtlinieneigenschaften verwalten (**Light Agent-Modus**).

Verbindung zum Integrationsserver

Die in diesem Abschnitt beschriebenen Befehle können nur ausgeführt 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 mit dem Integrationsserver

Parameter	Description
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 ein NetBIOS-Name, localhost oder 127.0.0.1 angegeben ist, wird die Verbindung zum Integrationsserver mit einem Fehler beendet.
Port	Port für die Verbindung zum Integrationsserver. Der Standardport ist 7271.

Wenn in Ihrer Infrastruktur ein Failover-Cluster von Integrationsservern auf Linux-Basis bereitgestellt ist, müssen Sie als Adresse und Port für die Verbindung zum Integrationsserver die Adresse und den Port des Load Balancers eingeben. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

Fenster "Prüfung des Integrationsserver-Zertifikats"

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 dem Integrationsserver mittels Administratorrechten hergestellt wurde, wird das Kennwort des 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 gelten nur, wenn Kaspersky Endpoint Security im Light Agent-Modus 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

Parameter	Description
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 angegebene 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 mehrere IP-Adressen oder vollständige Domänennamen der 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 Anwendung führen. Sie können in der Liste ausgewählte Adressen löschen, indem Sie auf die Schaltfläche **Löschen** klicken. Wenn die Option **Manuell angegebene 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 für die Option **SVM-Standort** den Wert **Ignorieren** festlegen. Bei einem beliebigen anderen angegebenen Wert kann der Light Agent keine Verbindung zur SVM herstellen.

Tag für die 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

Parameter	Description
Tag für die Verbindung 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 können Sie eine Zeichenkette von höchstens 255 Zeichen Länge eingeben. Sie können beliebige Zeichen außer dem Zeichen `;` verwenden. Das Feld ist verfügbar, wenn das Kontrollkästchen **Tag für die Verbindung** aktiviert ist.

Algorithmus der SVM-Auswahl

In diesem Fenster können Sie angeben, welchen Algorithmus zur SVM-Auswahl die Light Agents verwenden sollen, und die Einstellungen für die Verwendung des erweiterten Algorithmus zur SVM-Auswahl konfigurieren.

Algorithmus der SVM-Auswahl

Parameter	Description
Standardalgorithmus 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 gefunden werden, die für eine Verbindung geeignet sind, wählt der Light Agent die SVM aus, mit der die wenigsten Light Agents verbunden sind. Dabei bleibt die Platzierung der SVM in der virtuellen Infrastruktur unberücksichtigt. Diese Option ist standardmäßig ausgewählt.
Erweiteren 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.

Parameter	Description

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 einer virtuellen Infrastruktur auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).
	  • Die SVM befindet sich in derselben Servergruppe wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird).
	  • Die SVM befindet sich auf demselben Knoten wie die virtuelle Maschine mit installiertem Light Agent (in a virtual infrastructure Basis Dynamix Enterprise).
	  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 in demselben Hypervisor-Cluster bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).
	  • Die SVMs werden auf demselben OpenStack-Projekts bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack-Plattform oder VK Private Cloud ausgeführt wird).
	  • Die SVM befindet sich auf demselben Zone wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Basis Dynamix Enterprise).
	  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.
	• **Datencenter**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):
	  • Die SVM wird in demselben Rechenzentrum bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).
	  • Die SVM befindet sich in derselben Verfügbarkeitszone wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack-Plattform oder VK Private Cloud betrieben wird).
	  • Die SVM befindet sich in demselben Rechenzentrum wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Basis Dynamix Enterprise).
	  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.
	• **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 **Erweiteren 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. Dafür müssen Sie die für den Parameter **SVM-Standort** den Wert **Ignorieren** festlegen. Bei einem beliebigen anderen angegebenen Wert kann der Light Agent keine Verbindung zur SVM herstellen.

Schutz der Verbindung

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

Parameter	Description
Kanal für die Datenübertragung zwischen Light Agent und 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.

Bekannte Probleme und Einschränkungen

Einschränkungen des Programms

Kaspersky Endpoint Security wird in folgenden Fällen nicht unterstützt:

- Auf OSnova-Betriebssystemen im Modus der geschlossenen Softwareumgebung und im Modus des gehärteten Kernels.
- Auf Betriebssystemen auf Basis von Red Hat Enterprise Linux mit dem IMA-Subsystem.
- Auf Betriebssystemen auf Basis von Red Hat Enterprise Linux im FIPS-Modus.
- Auf Ubuntu-Betriebssystemen und Betriebssystemen auf Basis von SUSE Linux Enterprise Server mit dem System zur obligatorischen Zugriffskontrolle AppArmor.
- Mit Grsecurity-Sicherheitssystemen (auf allen Betriebssystemen).
- Bei Verwendung des seccomp-Mechanismus (auf allen Betriebssystemen).
- Bei Verwendung der Technologien WSL1 und WSL2 (auf allen Betriebssystemen).
- Bei Verwendung bestimmter Mount-Optionen für Dateisysteme (z. B. noexec, nosuid).
- Wenn Kaspersky Endpoint Security innerhalb eines Containers installiert ist.

Detection and Response-Lösungen funktionieren möglicherweise nicht ordnungsgemäß auf virtuellen Maschinen, die aus einem Image erstellt wurden, auf dem Kaspersky Endpoint Security für Linux installiert ist. Bei der Integration mit Detection and Response-Lösungen wird eine eindeutige ID (Sensor ID) des Computers verwendet. Das Programm generiert diese ID im Rahmen der Erstinstallation, und sie bleibt auch nach der Deinstallation des Programms erhalten. Beim Klonen eines Images übernimmt die virtuelle Maschine die Sensor ID, was dazu führen kann, dass Detection and Response-Lösungen mehrere virtuelle Maschinen als dasselbe Gerät identifizieren.

Einschränkungen des Programms bei bestimmten Architekturen

Das Programm unterliegt Einschränkungen bei der Ausführung auf den folgenden Prozessorarchitekturen:

Elbrus

- Light Agent-Modus: Wird nicht unterstützt.
- EDR-Agent-Modus: Wird nicht unterstützt.
- Schutz vor BadUSB-Angriffen: Funktioniert nicht.
- Exploit-Prävention: Funktioniert nicht.

- Schutz vor Web-Bedrohungen: Die heuristische Analyse ist bei der Untersuchung von Webseiten auf Phishing-Links nicht verfügbar.
- Integration mit Kaspersky Endpoint Detection and Response Optimum: Funktioniert nicht.
- Integration mit Kaspersky Endpoint Detection and Response Expert (cloud): Funktioniert nicht.
- Integration mit Kaspersky Endpoint Detection and Response (KATA): Funktioniert nicht.
- Integration mit Kaspersky Managed Detection and Response: Funktioniert nicht.
- Sandbox: Funktioniert nicht.
- KUMA-Integration: Funktioniert nicht.
- Untersuchung von Containern: Funktioniert nicht.
- Aktualisierbares Kernel-Modul: Nicht unterstützt.
- Grafische Benutzeroberfläche der Verwaltung: Benutzer können keine Dateien zur Untersuchung in der Sandbox einreichen, da die Sandbox-Komponente nicht unterstützt wird.

Einschränkungen des Programms auf einigen Betriebssystemen

Das Programm unterliegt Einschränkungen bei der Ausführung auf den folgenden Betriebssystemen:

Astra Linux Special Edition RUSB.10015-01 (operational update 1.5)

- Schutz vor BadUSB-Angriffen: Funktioniert nicht, da der Dienst systemd-logind im Betriebssystem fehlt.
- Die Beschränkung der CPU-Ressourcennutzung für die Aufgaben Schadsoftware-Untersuchung, Untersuchung wichtiger Bereiche, Inventarisierung und Untersuchung von Containern funktioniert nicht bei Kerneln vom Typ "4.2.0-23-generic".

CentOS 5.2 und 5.4

- Verhaltensanalyse: Es kann nicht garantiert werden, dass die Komponente ordnungsgemäß funktioniert, da das synchrone Abfangen von Prozessstarts nicht verfügbar ist.
- Schutz vor E-Mail-Bedrohungen: Funktioniert nicht.
- Schutz vor Web-Bedrohungen: Funktioniert nicht, da der TProxy-Mechanismus nicht unterstützt wird.
- Schutz vor Netzwerkbedrohungen: Funktioniert nicht, da der TProxy-Mechanismus nicht unterstützt wird.
- Schutz vor Verschlüsselung: Funktioniert nicht, da der TProxy-Mechanismus nicht unterstützt wird.
- Schutz vor BadUSB-Angriffen: Funktioniert nicht, da der Dienst systemd-logind im Betriebssystem fehlt.
- Untersuchung von Containern: Funktioniert nicht, da das Betriebssystem keine Container unterstützt.

- Gerätekontrolle: Der Nur-Lese-Modus für Geräte funktioniert nur, wenn das Gerät nach der Aktivierung des Modus im Programm verbunden wurde. Für Geräte, die vor der Aktivierung dieses Modus verbunden wurden, bleibt der Zugriffsmodus unverändert.
- Programmkontrolle: Funktioniert nicht, da die fanotify-Technologie, die für das synchrone Abfangen des Prozessstarts erforderlich ist, nicht unterstützt wird.
- Firewall-Verwaltung: Funktioniert nicht, da das Hinzufügen von Ketten zu iptables nicht unterstützt wird.
- Web-Kontrolle: Funktioniert nicht, da der TProxy-Mechanismus nicht unterstützt wird.
- Aktualisierbares Kernel-Modul: Nicht unterstützt.
- Netzwerkisolation: Funktioniert nicht, da der TProxy-Mechanismus nicht unterstützt wird.
- Ausführungsprävention für Objekte funktioniert nicht, da der Prozessstart nicht synchron abgefangen wird.
- Integration mit Kaspersky Endpoint Detection and Response Optimum: Funktioniert nicht.
- Integration mit Kaspersky Endpoint Detection and Response Expert (cloud): Funktioniert nicht.
- Integration von Kaspersky Endpoint Detection and Response (KATA): Die eBPF-Telemetriedatenquelle ist nicht verfügbar.
- Integration von Kaspersky Managed Detection and Response: Die auditd-Telemetriedatenquelle ist nicht verfügbar.
- Grafische Benutzeroberfläche: Funktioniert nicht, da die Bibliothek libxcb im Betriebssystem fehlt.
- Kaspersky Security Center Administrationsagent: Erfordert eine zusätzliche Gerätekonfiguration. Siehe die Hilfe zu Kaspersky Security Center.
- Installation/Deinstallation: Das Programm ist in diesen Versionen des Betriebssystems nicht mit SELinux kompatibel. Mögliche Lösung: SELinux in den nicht blockierenden Modus (Permissive-Modus) versetzen, SELinux deaktivieren oder SELinux manuell konfigurieren.
- Schadsoftware-Untersuchung: In Betriebssystemen mit glibc-Versionen vor 2.11 werden Dateien, die sich in Verzeichnissen mit einer Pfadlänge von mehr als 4096 Zeichen befinden, nicht desinfiziert oder gelöscht.
- Die Beschränkung der CPU-Ressourcennutzung für die Aufgaben „Schadsoftware-Untersuchung“, „Untersuchung wichtiger Bereiche“, „Inventarisierung“ und „Untersuchung von Containern“ funktioniert nicht.
- Der Light Agent-Modus wird nicht unterstützt. Daher sind die Einstellungen KSVLA_MODE, SERVER_MODE und VDI_MODE bei der Installation des Programms nicht anwendbar.
- Der Programmbetrieb im EDR-Agent-Modus wird nicht unterstützt.
- Das Programm wird in der Kaspersky Security Center Cloud Console nicht unterstützt.
- Das Programm unterstützt keine Dateisysteme, die auf der FUSE-Technologie basieren.
- Statistiken zu den am häufigsten untersuchten Dateien werden nicht erfasst.
- In einigen Fällen können die im Rahmen der Integration mit Kaspersky Endpoint Detection and Response (KATA) übertragenen Telemetriedaten unvollständige Informationen über Ereignisse aus Systemereignisprotokollen enthalten.

CentOS 6.4 und 6.6

- Verhaltensanalyse: Es kann nicht garantiert werden, dass die Komponente ordnungsgemäß funktioniert, da das synchrone Abfangen von Prozessstarts nicht verfügbar ist.
- Schutz vor Web-Bedrohungen: Das Abfangen des IPv6-Datenverkehrs funktioniert nicht.
- Schutz vor Netzwerkbedrohungen: Das Abfangen des IPv6-Datenverkehrs funktioniert nicht.
- Schutz vor Verschlüsselung: Das Abfangen des IPv6-Datenverkehrs funktioniert nicht.
- Schutz vor BadUSB-Angriffen: Funktioniert nicht, da der Dienst systemd-logind im Betriebssystem fehlt.
- Untersuchung von Containern: Funktioniert nicht, da das Betriebssystem keine Container unterstützt.
- Programmkontrolle: Funktioniert nicht, da die fanotify-Technologie, die für das synchrone Abfangen des Prozessstarts erforderlich ist, nicht unterstützt wird.
- Firewall-Verwaltung: IPv6-Regeln der Firewall funktionieren nicht.
- Web-Kontrolle: Das Abfangen des IPv6-Datenverkehrs funktioniert nicht.
- Aktualisierbares Kernel-Modul: Nicht unterstützt.
- Ausführungsprävention für Objekte funktioniert nicht, da der Prozessstart nicht synchron abgefangen wird.
- Kaspersky Endpoint Detection and Response Optimum: Die Entwicklungskette der Bedrohung bildet keine Netzwerkaktivität ab, da keine TProxy-Unterstützung vorhanden ist. Es sind nur Telemetriedatenereignisse zu Dateivorgängen verfügbar. Die Ausführungsprävention für Objekte funktioniert nicht, da das synchrone Abfangen des Prozessstarts nicht verfügbar ist.
- Integration mit Kaspersky Endpoint Detection and Response Expert (cloud): Funktioniert nicht.
- Integration von Kaspersky Endpoint Detection and Response (KATA): Die eBPF-Telemetriedatenquelle ist nicht verfügbar.
- Integration von Kaspersky Managed Detection and Response: Die auditd-Telemetriedatenquelle ist nicht verfügbar.
- Kaspersky Security Center Administrationsagent: Erfordert eine zusätzliche Gerätekonfiguration. Siehe die Hilfe zu Kaspersky Security Center.
- Installation/Deinstallation: Das Programm ist in diesen Versionen des Betriebssystems nicht mit SELinux kompatibel. Mögliche Lösung: SELinux in den nicht blockierenden Modus (Permissive-Modus) versetzen, SELinux deaktivieren oder SELinux manuell konfigurieren.
- Schadsoftware-Untersuchung: In Betriebssystemen mit glibc-Versionen vor 2.11 werden Dateien, die sich in Verzeichnissen mit einer Pfadlänge von mehr als 4096 Zeichen befinden, nicht desinfiziert oder gelöscht.
- Der Programmbetrieb im Light Agent-Modus und im EDR-Agent-Modus wird nicht unterstützt.
- Das Programm wird in der Kaspersky Security Center Cloud Console nicht unterstützt.

- Statistiken zu den am häufigsten untersuchten Dateien werden nicht erfasst.
- In einigen Fällen können die im Rahmen der Integration mit Kaspersky Endpoint Detection and Response (KATA) übertragenen Telemetriedaten unvollständige Informationen über Ereignisse aus Systemereignisprotokollen enthalten.

Einschränkungen im Zusammenhang mit den Werten der ptrace-Einstellung

Die Werte der Einstellung `kernel.yama.ptrace_scope` des Betriebssystems können sich auf Kaspersky Endpoint Security auswirken:

- 1 (eingeschränktes ptrace). Ein Prozess kann nur eine Verbindung mit Prozessen herstellen, die er selbst gestartet hat. Für die Verbindung mit anderen Prozessen ist eine spezielle Berechtigung erforderlich. Die Funktionalität des Programms ist wie folgt eingeschränkt:
  - Die Komponente Verhaltensanalyse kann die Umgebungsparameter von Prozessen nicht abrufen.
  - Auf Betriebssystemen mit einer Kernel-Version höher als 5.7 kann die Komponente Programmkontrolle die Befehlszeilenargumente und Umgebungsvariablen von Prozessen nicht lesen, da das Lesen von /proc/<pid>/syscall und /proc/<pid>/mem verboten ist. Auf Betriebssystemen mit Kernel-Version 5.0 kann die Komponente Programmkontrolle nicht ordnungsgemäß funktionieren.
  - Die Untersuchung des Prozessspeichers und des Kernel-Speichers funktioniert in Untersuchungsaufgaben nicht, da das Lesen von /proc/<pid>/mem verboten ist.
  - Die YARA-Untersuchung des Prozessspeichers kann nicht garantiert werden, da das Lesen von /proc/<pid>/mem nicht erlaubt ist.
- 2 (administratives ptrace). Nur Prozesse mit CAP_SYS_PTRACE-Berechtigungen (normalerweise root) können ptrace verwenden oder Zugriff auf einen Prozess in /proc (/proc/<pid>/mem) erhalten. Die Problembehandlung ist dadurch eingeschränkt, dass Absturzabbilder für Benutzerprozesse (wie kesl-control und kesl-gui) nicht funktionieren, während Abbilder für den kesl-Prozess selbst funktionieren.
- 3 (ptrace verboten): ptrace ist auf Betriebssystemebene vollständig verboten. Die Funktionalität des Programms ist wie folgt eingeschränkt:
  - Absturzabbilder funktionieren weder für den kesl-Prozess noch für Benutzerprozesse (wie kesl-control und kesl-gui).
  - Die Komponente Verhaltensanalyse kann die Umgebungsparameter von Prozessen nicht abrufen.
  - Die Komponente Programmkontrolle wird nicht unterstützt.

- Da das Verzeichnis /proc/<pid>/mem nicht gelesen werden kann:
  - Die Untersuchung des Prozessspeichers und des Kernel-Speichers funktioniert in Untersuchungsaufgaben nicht.
  - Die Aufgaben „Speicherabbild abrufen“ und „Prozessspeicherabbild abrufen“ funktionieren bei der Integration mit Detection and Response-Lösungen nicht.
  - Es kann nicht garantiert werden, dass YARA-Untersuchungen des Prozessspeichers im Modus der obligatorischen Zugriffskontrolle bei der Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) funktionieren.

Einschränkungen des aktualisierbaren Kernel-Moduls

Das aktualisierbare Kernel-Modul unterstützt die folgenden Kernel-Varianten und -Versionen nicht:

Ubuntu

- `*-kvm`
- `*-gkeop 5.15.0-100[1234] (bionic/jammy)`
- `focal 5.10.0-1002-oem`
- `noble 6.8.0-1014-ibm`
- `*-realtime`
- `*-uc-*`
- `kinetic 5.18.0-100(1|2)-(ibm|gcp|oracle)`

Astra

- `6.1.90-1-generic-*, 6.6.28-1-generic-*`
- `*-hardened`

Debian

- `*-rt`
- `5.14.0-1-(cloud-amd64|amd64)-5.14.6-2`
- `6.1.0-36-(cloud-amd64|amd64)-6.1.139-1`
- `6.5.0-5-*amd64-6.5.13-1`
- `6.6.*`

RED OS 7.3.

- `kernel-ml-5.14.9-1.el7`

RED OS 8.0

- `6.6.26-1.red80`
- `6.6.34-1.red80`
- `6.6.51-1.red80`
- `6.6.76-1.red80`
- `6.6.6-1.red80`

Einschränkungen bei der Verwendung der eBPF-Technologie

Um die eBPF-Technologie zum Abfangen des Netzwerkverkehrs zu verwenden, benötigen Sie einen Linux-Kernel der Version 4.18 oder höher, der mit den folgenden Optionen kompiliert wurde:

- `CONFIG_DEBUG_INFO_BTF=y` oder `m` (Unterstützung für eBPF mit BTF)
- `CONFIG_KPROBES= y`
- `CONFIG_TRACEPOINTS=y`
- `CONFIG_FSNOTIFY=y`

Um eBPF beim Integrieren von Detection and Response-Lösungen zum Senden von Telemetriedaten zu verwenden, benötigen Sie einen Linux-Kernel der Version 4.18 oder höher, der mit den folgenden Optionen kompiliert wurde:

- `CONFIG_BPF=y`
- `CONFIG_BPF_SYSCALL=y`
- `CONFIG_TRACEPOINTS=y`
- `CONFIG_KPROBES=y`
- `CONFIG_KPROBES_ON_FTRACE=y`
- `CONFIG_KRETPROBES=y`
- `CONFIG_HAVE_SYSCALL_TRACEPOINTS=y`
- `CONFIG_FTRACE=y`
- `CONFIG_FUNCTION_TRACER=y`

- `CONFIG_DYNAMIC_FTRACE=y`
- `CONFIG_DYNAMIC_FTRACE_WITH_REGS=y`
- `CONFIG_FTRACE_SYSCALLS=y`
- `CONFIG_KPROBE_EVENTS=y`
- `CONFIG_FSNOTIFY=y`

Besonderheiten

- Das Programm kann nicht gleichzeitig im Light Agent-Modus und im EDR Agent-Modus verwendet werden.
- In Betriebssystemen mit auditd 3.0.7 und Linux-Kernel 4.18 kann die Verwendung der Komponente Verhaltensanalyse dazu führen, dass das Programm und SSH-Verbindungen einfrieren.
- Auf Betriebssystemen mit Kylin Desktop V10 SP1 2303 kann die Komponente Verhaltensanalyse dazu führen, dass das Betriebssystem einfriert. Zur Behebung dieses Problems empfehlen wir, den Kernel des Betriebssystems zu aktualisieren.
- Für Regeln der Programmkontrolle wird in der Web Console die Einstellung **Für andere Benutzer verbieten** angezeigt. Diese Einstellung wird vom Programm nicht verwendet und hat keinen Einfluss auf die Funktionsweise der Regeln der Programmkontrolle.

Besonderheiten für den Light Agent-Modus

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

- 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.
- Interagiert Kaspersky Endpoint Security über den KSN-Proxyserver mit den Servern von KSN. Wird die direkte Interaktion mit KSN nicht unterstützt.
- Wird die Verwendung des Proxyservers der Anwendung bei einer Verbindung zum Integrationsserver, zu den SVMs oder KSN-Servern nicht unterstützt.

Besonderheiten für den EDR Agent-Modus

Wenn Kaspersky Endpoint Security im EDR Agent-Modus verwendet wird, ist nur ein begrenzter Teil der Programmkomponenten und Aufgaben verfügbar. Nach der Installation werden die Anwendungseinstellungen wie folgt konfiguriert:

- Die Integration von Kaspersky Endpoint Detection and Response Expert (cloud) wird nicht unterstützt.
- Vollständig konfigurierbare Komponenten, welche die Integration mit den Detection and Response gewährleisten:
  - EDR Expert (on-premise)
  - NDR (KATA)

  Diese Komponenten sind standardmäßig deaktiviert. Sie müssen sie aktivieren, damit das Programm im EDR Agent-Modus funktioniert. Sie können die Integrationsparameter, einschließlich der Funktion zur Ausführungsprävention von Objekten, konfigurieren.
- Der Zugriff auf Dateien wird während der Untersuchung nicht blockiert: das Kontrollkästchen **Zugriff auf den Dateien während der Untersuchung blockieren** (`FileBlockDuringScan=No`) ist deaktiviert. Diese Einstellung kann geändert werden, wird aber auf dem geschützten Gerät nicht angewendet.
- Die Komponenten "Schutz vor bedrohlichen Dateien" und "Schutz vor Verschlüsselung" sind im Modus mit eingeschränktem Funktionsumfang verfügbar: Wenn eine Bedrohung erkannt wird, versuchen die Komponenten nicht, schädliche Objekte zu löschen, Zugriff zu verbieten oder Anwendungsaktivitäten zu blockieren. Stattdessen senden sie lediglich die Information über eine erkannte Bedrohung an die Server, welche die Integration mit den Detection and Response-Lösungen gewährleisten.

  Sie können die Komponenten "Schutz vor bedrohlichen Dateien" und "Schutz vor Verschlüsselung" aktivieren, deaktivieren und deren Parameter mit Ausnahme der Aktion beim Erkennen von Bedrohungen konfigurieren. Die folgenden Einstellungen werden auf dem geschützten Gerät nicht angewendet:
  - Komponente "Schutz vor bedrohlichen Dateien": **Aktion beim Erkennen von Bedrohungen** – **Überspringen** (`ActionOnThreat=Skip`).
  - Komponente "Schutz vor Verschlüsselung": **Aktion beim Erkennen einer Verschlüsselung** – **Informieren** (`ActionOnDetect=Notify`).
- Die Komponente "Verhaltensanalyse" ist vollständig konfigurierbar.
- Alle anderen Schutz- und Kontrollkomponenten sind deaktiviert und stehen nicht zur Verwaltung zur Verfügung.

Bei der Integration in Kaspersky Endpoint Detection and Response Expert (on-premise) oder in Kaspersky Endpoint Detection and Response (KATA) kann Kaspersky Endpoint Security im Rahmen einer Aktion zur Reaktion auf Bedrohungen den Start ausführbarer Dateien und Skripte auf dem Gerät kontrollieren. Die Funktionen der Ausführungsprävention für Objekte sind mit folgenden Einschränkungen verfügbar:

- Wenn ein Skript von einem Interpreter aus gestartet wird, hat die Anwendung keine Kontrolle über den Start des Skripts.
- Die Anwendung hat keinen Einfluss auf das Öffnen von Dateien für Office-Anwendungen auf dem Gerät.

Anfrage an den Technischen Support

Sollten Sie in der Dokumentation und oder in anderen Informationsquellen für die Anwendung 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 für jede Version von Kaspersky Endpoint Security während des Lebenszyklus dieser Version (siehe Seite zum Lebenszyklus der Anwendung). Bitte beachten Sie die Support-Regeln, bevor Sie sich an den Technischen Support wenden.

Eine Kontaktaufnahme mit den Support-Experten ist auf folgende Weise möglich:

- Aufrufen der Webseite des Technische Supports
- Anfrage an den Technischen Support von Kaspersky über das Portal Kaspersky CompanyAccount.

Technischer Support über Kaspersky CompanyAccount

Kaspersky CompanyAccount – Ein Webdienst für Unternehmen, die Anwendungen von Kaspersky verwenden. Kaspersky CompanyAccount ermöglicht es Organisationen, die Kaspersky-Programme verwenden, den Technischen Support von Kaspersky per E-Mail-Anfrage zu kontaktieren. Auf dem Portal können Sie neue Anfragen erstellen, ihren Fortschritt überwachen und den Verlauf der Anfragebearbeitung speichern.

Registrieren Sie alle Mitarbeiter Ihres Unternehmens unter einem einzigen Benutzerkonto in Kaspersky CompanyAccount. Dadurch können Sie elektronische Anfragen an Kaspersky zentral verwalten und den Zugriff Ihrer Benutzer auf Kaspersky CompanyAccount kontrollieren.

Das Portal Kaspersky CompanyAccount ist in den folgenden Sprachen verfügbar:

- Deutsch
- Spanisch
- Italienisch
- Deutsch
- Polnisch
- Portugiesisch
- Russisch
- Französisch
- Japanisch

Weitere Informationen zu Kaspersky CompanyAccount finden Sie auf der Website des Technischen Supports von Kaspersky CompanyAccount.

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 Protokolldatei* 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 Anwendungskomponenten anfordern.

Während der Diagnose werden Sie möglicherweise von Spezialisten des Technischen Supports dazu aufgefordert, die folgenden Einstellungen der Anwendung zu ändern:

- Die Funktionalität zum Abrufen erweiterter Diagnoseinformationen aktivieren.
- Die Ausführung einzelner Anwendungskomponenten, 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.

So aktivieren und konfigurieren Sie die Erstellung von Protokolldateien

Mit einer *Protokolldatei* von Kaspersky Endpoint Security können Sie die schrittweise Ausführung von Anwendungsbefehlen verfolgen und erkennen, in welcher Phase der Anwendungsausführung ein Fehler auftritt.

Standardmäßig werden keine Protokolldateien der Anwendung erstellt. Sie können die Erstellung von Protokolldateien aktivieren oder deaktivieren und die Protokollierungsstufe über die Befehlszeile, in den allgemeinen Programmeinstellungen oder in der grafischen Benutzeroberfläche auswählen.

Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center verwalten, können Sie die Einstellungen für die Protokollierung in den Einstellungen der Richtlinie von Kaspersky Endpoint Security entweder über die Web Console oder die Verwaltungskonsole konfigurieren.

So verwalten Sie Protokollierungseinstellungen in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Allgemeine Einstellungen** → **Technischer Support** und sehen Sie unter **Protokollierungseinstellungen** nach.
5. Wenn Sie das Verzeichnis ändern möchten, in dem die Protokolldateien des Programms standardmäßig gespeichert werden, geben Sie im Feld **Pfad für Ablaufverfolgungsdateien** das Verzeichnis zum Speichern der Protokolldateien an. Standardwert: /var/log/kaspersky/kesl. Für den Zugriff auf das Standardverzeichnis zum Speichern von Protokolldateien sind Root-Rechte erforderlich. Wenn Sie ein anderes Verzeichnis angeben, stellen Sie sicher, dass nur root Lese- und Schreibberechtigungen für dieses Verzeichnis hat (Berechtigungen `700` oder `rwx--------`).
6. Geben Sie bei Bedarf im Feld **Maximale Größe einer Protokolldatei (MB)** die maximale Größe einer Protokolldatei des Programms (in Megabyte) an. Standardwert: 500.
7. Geben Sie bei Bedarf im Feld **Maximale Anzahl der Protokolldateien** die maximale Anzahl der Protokolldateien des Programms an. Standardwert: 10.
8. Speichern Sie die vorgenommenen Änderungen.
9. Starten Sie das Programm neu, damit die Protokollierungseinstellungen übernommen werden.

So verwalten Sie Protokollierungseinstellungen 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. Wechseln Sie zum Abschnitt **Allgemeine Einstellungen** → **Programmeinstellungen**.
5. Klicken Sie unter **Einstellungen für Protokollierung und Dumps** auf **Konfigurieren**.
6. Das Fenster **Einstellungen für Protokollierung und Dumps** wird geöffnet.
7. Wenn Sie das Verzeichnis ändern möchten, in dem die Protokolldateien des Programms standardmäßig gespeichert werden, geben Sie im Feld **Pfad zum Verzeichnis der Protokolldateien** das Verzeichnis zum Speichern der Protokolldateien an. Standardwert: /var/log/kaspersky/kesl. Für den Zugriff auf das Standardverzeichnis zum Speichern von Protokolldateien sind Root-Rechte erforderlich. Wenn Sie ein anderes Verzeichnis angeben, stellen Sie sicher, dass nur root Lese- und Schreibberechtigungen für dieses Verzeichnis hat (Berechtigungen `700` oder `rwx--------`).

8. Geben Sie bei Bedarf im Feld **Maximale Größe der Protokolldatei (MB)** die maximale Größe einer Protokolldatei des Programms (in Megabyte) an. Standardwert: 500.

9. Geben Sie bei Bedarf im Feld **Maximale Anzahl von Protokolldateien** die maximale Anzahl von Protokolldateien an, die das Programm erstellen kann. Standardwert: 10.

10. Klicken Sie im Fenster **Einstellungen für Protokollierung und Dumps** auf **OK**.

11. Klicken Sie auf **Übernehmen**.

12. Starten Sie das Programm neu, damit die Protokollierungseinstellungen übernommen werden.

So aktivieren Sie die Protokollierung und verwalten Protokollierungseinstellungen über die Befehlszeile

Über die Befehlszeile können Sie die Protokollierung mithilfe der Einstellungen `TraceLevel`, `TraceFolder`, `TraceMaxFileCount` und `TraceMaxFileSize` in den allgemeinen Programmeinstellungen konfigurieren. Sie können die Werte der Einstellungen mithilfe von Befehlszeilenschaltern oder einer Konfigurationsdatei ändern, die alle allgemeinen Programmeinstellungen enthält.

Gehen Sie wie folgt vor, um eine Protokolldatei zu erstellen und die Protokollierungseinstellungen über die Befehlszeile anzupassen:

1. Aktivieren Sie die Erstellung einer Protokolldatei und wählen Sie eine Protokollierungsstufe aus:

   ```
   kesl-control --set-app-settings TraceLevel=Detailed | MediumDetailed | NotDetailed
   ```

   Wobei gilt:

   - `Detailed` – detaillierteste Protokolldateien erstellen.
   - `MediumDetailed` – Protokolldatei mit Info- und Fehlermeldungen erstellen.
   - `NotDetailed` – Protokolldatei mit Fehlermeldungen erstellen.

2. Wenn Sie das Verzeichnis ändern möchten, in dem die Protokolldateien des Programms standardmäßig gespeichert werden, geben Sie das Verzeichnis zum Speichern der Protokolldateien an:

   ```
   kesl-control --set-app-settings TraceFolder=<path to trace files directory>
   ```

   Dabei ist `<path to trace files directory>` der Pfad zum Verzeichnis, in dem Protokolldateien gespeichert werden. Standardwert: /var/log/kaspersky/kesl. Für den Zugriff auf das Standardverzeichnis zum Speichern von Protokolldateien sind Root-Rechte erforderlich. Wenn Sie ein anderes Verzeichnis angeben, stellen Sie sicher, dass nur root Lese- und Schreibberechtigungen für dieses Verzeichnis hat (Berechtigungen `700` oder `rwx--------`).

3. Geben Sie bei Bedarf die maximale Anzahl von Protokolldateien an:

   ```
   kesl-control --set-app-settings TraceMaxFileCount=<number of application trace files>
   ```

   Dabei ist `<number of application trace files>` die maximale Anzahl von Protokolldateien des Programms. Mögliche Werte: 1 bis 10000. Standardwert: 10.

4. Geben Sie bei Bedarf die maximale Größe einer Protokolldatei des Programms (in Megabyte) an:

```
kesl-control --set-app-settings TraceMaxFileSize=<size of an application trace file>
```

Dabei ist `<size of an application trace file>` die maximale Größe einer Protokolldatei in Megabyte. Mögliche Werte: 1 bis 1000. Standardwert: 500.

Nach dem Ändern der Werte für die Parameter `TraceFolder`, `TraceMaxFileCount` und `TraceMaxFileSize` müssen Sie die Anwendung neu starten.

```
Um die Erstellung von Protokolldateien zu deaktivieren, führen Sie den folgenden Befehl aus:
```

```
kesl-control --set-app-settings TraceLevel=None
```

So aktivieren Sie die Protokollierung und verwalten Protokollierungseinstellungen über die grafische Benutzeroberfläche

Für die Erstellung der Protokolldatei und die Konfiguration der Detailstufe sind Benutzerberechtigungen mit Administratorrolle (admin) erforderlich.

1. Öffnen Sie das Hauptfenster der grafischen Benutzeroberfläche des Programms.
2. Klicken Sie im unteren Bereich des Hauptfensters der Anwendung 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 **Stufe** den Detaillierungsgrad der Protokolldatei aus:

   - **Diagnose (300)** – nur Fehlermeldungen.
   - **Informativ (700)** – Informations- und Fehlermeldungen.
   - **Debuggen (800)** – detaillierte Protokolldatei.

   Wir empfehlen, den erforderlichen Detaillierungsgrad mit einem Spezialisten des Technischen Supports von Kaspersky abzuklären. Die Standardeinstellung ist **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.

Sie können außerdem die Erstellung von Protokolldateien des Watchdog-Servers aktivieren und konfigurieren.

So aktivieren Sie die Protokollierung und verwalten die Protokollierungseinstellungen des Watchdog-Servers über die Befehlszeile

In der Befehlszeile können Sie die Protokollierung des Watchdog-Servers mithilfe der `WdTraceLevel`-Einstellungen in den allgemeinen Programmeinstellungen konfigurieren. Sie können die Werte der Einstellungen mithilfe von Befehlszeilenoptionen oder einer Konfigurationsdatei ändern, die alle allgemeinen Programmeinstellungen enthält.

```
Erstellen Sie die Protokolldatei des Watchdog-Servers und konfigurieren Sie die Protokollierungseinstellungen über die Befehlszeile
```

```
kesl-control --set-app-settings WdTraceLevel=Detailed | MediumDetailed | NotDetailed | Product
```

Wobei gilt:

- `Detailed` – detaillierteste Protokolldateien erstellen.
- `MediumDetailed` – Protokolldatei mit Info- und Fehlermeldungen erstellen.
- `NotDetailed` – Protokolldatei mit Fehlermeldungen erstellen.
- `Product` – Legen Sie den Wert gleich dem Wert der Einstellung `TraceLevel` in den allgemeinen Programmeinstellungen fest. Wenn `TraceLevel=None`, wird keine Protokolldatei erstellt.

```
Deaktivieren Sie die Erstellung der Protokolldatei des Watchdog-Servers und konfigurieren Sie die Protokollierungseinstellungen über die Befehlszeile
```

```
kesl-control --set-app-settings WdTraceLevel=None
```

Standardmäßig werden die erstellten Protokolldateien im Verzeichnis /var/log/kaspersky/kesl/ gespeichert. Für den Zugriff auf dieses Verzeichnis sind Root-Rechte erforderlich. Sie können ein anderes Verzeichnis zum Speichern von Protokolldateien angeben. Wenn Sie ein anderes Verzeichnis angeben, stellen Sie sicher, dass nur root Lese- und Schreibberechtigungen für dieses Verzeichnis hat (Berechtigungen `700` oder `rwx--------`).

Die Protokolldateien der grafischen Benutzeroberfläche und des Befehlszeilenprogramms kesl-control werden im Verzeichnis /var/log/kaspersky/kesl-user gespeichert. Um die Erstellung dieser Protokolldateien zu aktivieren, müssen Sie die Umgebungsvariable LFS_ENABLE_ALL_COMPONENTS_LOGGING setzen.

Zum Speichern von Protokolldateien benötigt das Programm zusätzlich zu dem in den Mindestanforderungen an die Hardware angegebenen Speicherplatz weiteren Speicherplatz auf dem Datenträger.

Protokolldateien werden auf dem Gerät gespeichert, solange die Anwendung verwendet wird. Bei der Deinstallation der Anwendung 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.

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-Plug-ins für die Verwaltung 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 Anwendung, 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-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-Plug-in anlegen. Für weitere ausführliche Informationen zum Anlegen von Protokolldateien können Sie sich an den Technischen Support wenden.

Alle erstellten Protokolldateien des MMC-Plug-ins befinden sich in dem Ordner, den der Benutzer beim Festlegen der Registrierungsschlüssel angegeben hat.

Protokolldateien des Web-Plug-ins für die Verwaltung

Wenn Sie Web Console zur Verwaltung von Kaspersky Endpoint Security verwenden, können Informationen über Ereignisse während der Ausführung des Web-Plug-ins für die Verwaltung in den Protokolldateien des Web-Plug-ins aufgezeichnet werden.

Protokolldateien des Web-Plug-ins werden automatisch erstellt, wenn die Protokollierung von Aktivitäten der Web Console im Installationsassistenten der Web Console aktiviert ist (weitere Informationen finden Sie in der Hilfe zu Kaspersky Security Center).

Die Protokolldateien des Web-Plug-ins werden im Installationsordner der Web Console im Unterordner "logs" gespeichert.

Inhalt von Protokolldateien des Programms

Die Protokolldateien enthalten die folgenden allgemeinen Informationen:

- Zeitpunkt des Auftretens des Ereignisses
- Nummer des ausführenden Threads
- Anwendungskomponente, die das Ereignis verursacht hat
- Signifikanz des Ereignisses (informatives Ereignis, Warnung, kritisches Ereignis, Fehler)
- Eine Beschreibung des Ereignisses, bei dem ein Befehl von einer Anwendungskomponente ausgeführt wird, und das Ergebnis der Ausführung dieses Befehls

Protokolldateien können zusätzlich zu den allgemeinen Daten die folgenden Informationen enthalten:

- Status der Anwendungskomponenten und Daten zu ihrer Ausführung
- Daten zur Benutzeraktivität in der Anwendung
- 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 Anwendungsdatenbanken)
- Daten, die von KATA-Servern, OSMP-Servern, NDR-Servern und Servern, welche die Interaktion mit Sandbox ermöglichen, abgerufen 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 Anwendung erforderlich sind

Inhalt der Protokolldateien der Verwaltungs-Plug-ins

Protokolldateien von Verwaltungs-Plug-ins enthalten die folgenden allgemeinen Daten:

- Zeitpunkt des Auftretens des Ereignisses
- Nummer des ausführenden Threads
- Anwendungskomponente, die das Ereignis verursacht hat
- Signifikanz des Ereignisses (informatives Ereignis, Warnung, kritisches Ereignis, Fehler)
- Eine Beschreibung des Ereignisses, bei dem ein Befehl von einer Anwendungskomponente ausgeführt wird, und das Ergebnis der Ausführung dieses Befehls

Neben allgemeinen Daten können Protokolldateien von Verwaltungs-Plug-ins 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.
- Benutzername und Kennwort für den Internet-Proxyserver.

So aktivieren und konfigurieren Sie die Erstellung von Dump-Dateien

Eine *Dump-Datei* enthält alle Informationen zum Arbeitsspeicher der Prozesse von Kaspersky Endpoint Security zum Zeitpunkt der Erstellung der Dump-Datei.

Dump-Dateien können persönliche Daten enthalten. Es wird empfohlen, die Informationen bis zu ihrer Übermittlung an Kaspersky vor unbefugtem Zugriff zu schützen.

Standardmäßig werden keine Dump-Dateien erstellt. Sie können die Dump-Erstellung bei Programmfehlern aktivieren oder 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 über die Web Console oder die Verwaltungskonsole aktivieren, deaktivieren und konfigurieren.

Wenn Sie das Programm über die Befehlszeile verwalten, können Sie die Dump-Erstellung über die allgemeinen Programmeinstellungen 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`.

So aktivieren und konfigurieren Sie die Dump-Erstellung in der Web Console

So aktivieren und konfigurieren Sie die Dump-Erstellung in der Web Console:

1. Wählen Sie im Hauptfenster der Web Console **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wechseln Sie im Abschnitt **Allgemeine Einstellungen** → **Technischer Support** zu **Debug-Informationen**.
5. Wenn Sie möchten, dass beim Absturz des Programms eine Dump-Datei erstellt wird, aktivieren Sie den Umschalter **Dump-Erstellung AKTIVIERT**.
6. Wenn Sie das Verzeichnis ändern möchten, in dem die Dump-Dateien des kesl-Prozesses standardmäßig gespeichert werden, geben Sie im Feld **Pfad für Code-Dumps** das Verzeichnis zum Speichern von Dump-Dateien an. Standardwert: /var/opt/kaspersky/kesl/common/dumps. Für den Zugriff auf das Standardverzeichnis zum Speichern von Dump-Dateien sind Root-Rechte erforderlich. Wenn Sie ein anderes Verzeichnis angeben, stellen Sie sicher, dass nur root Lese- und Schreibberechtigungen für dieses Verzeichnis hat (Berechtigungen `700` oder `rwx--------`).
7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren und konfigurieren Sie die Dump-Erstellung in der Verwaltungskonsole

So aktivieren und konfigurieren Sie die Dump-Erstellung 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. Wechseln Sie zum Abschnitt **Allgemeine Einstellungen** → **Programmeinstellungen**.
5. Klicken Sie unter **Einstellungen für Protokollierung und Dumps** auf **Konfigurieren**.
6. Das Fenster **Einstellungen für Protokollierung und Dumps** wird geöffnet.
7. Wenn Sie möchten, dass beim Absturz des Programms eine Dump-Datei erstellt wird, aktivieren Sie das Kontrollkästchen **Dump-Datei erstellen, wenn das Programm abstürzt**.

8. Wenn Sie das Verzeichnis ändern möchten, in dem die Dump-Dateien des kesl-Prozesses standardmäßig gespeichert werden, geben Sie im Feld **Pfad zum Verzeichnis der Dump-Dateien** das Verzeichnis zum Speichern von Dump-Dateien an. Standardwert: /var/opt/kaspersky/kesl/common/dumps. Für den Zugriff auf das Standardverzeichnis für Dump-Dateien sind Root-Berechtigungen erforderlich (Berechtigungen `700` oder `rwx--------`). Wenn Sie ein anderes Verzeichnis angeben, stellen Sie sicher, dass nur der Benutzer root Lese- und Schreibberechtigungen für dieses Verzeichnis hat.

9. Klicken Sie im Fenster **Einstellungen für Protokollierung und Dumps** auf **OK**.

10. Klicken Sie auf **Übernehmen**.

So aktivieren und konfigurieren Sie die Dump-Erstellung über die Befehlszeile

Über die Befehlszeile können Sie die Dump-Erstellung mithilfe der Einstellungen `CoreDumps` und `CoreDumpsPath` aus den allgemeinen Programmeinstellungen aktivieren, deaktivieren und konfigurieren.

So aktivieren und konfigurieren Sie die Dump-Erstellung:

1. Führen Sie den folgenden Befehl aus, um die Dump-Erstellung zu aktivieren:

   ```
   kesl --set-app-settings CoreDumps=Yes
   ```

2. Wenn Sie das Verzeichnis ändern möchten, in dem Dump-Dateien gespeichert werden, geben Sie den Pfad zum Verzeichnis in der Einstellung `CoreDumpsPath` an.

   ```
   kesl --set-app-settings CoreDumpsPath=<path to directory with dump files>
   ```

   Dabei steht `<path to directory with dump files>` für den Pfad zum Verzeichnis, in dem die Dump-Dateien gespeichert werden. Standardwert: /var/opt/kaspersky/kesl/common/dumps. Für den Zugriff auf das Standardverzeichnis für Dump-Dateien sind Root-Berechtigungen erforderlich (Berechtigungen `700` oder `rwx--------`). Wenn Sie ein anderes Verzeichnis angeben, stellen Sie sicher, dass nur der Benutzer root Lese- und Schreibberechtigungen für dieses Verzeichnis hat.

Um die Dump-Erstellung zu deaktivieren, führen Sie den folgenden Befehl aus:

```
kesl --set-app-settings CoreDumps=No
```

Wenn Sie die Dump-Erstellung aktiviert haben, werden Dump-Dateien standardmäßig in den folgenden Verzeichnissen gespeichert:

- /var/opt/kaspersky/kesl/common/dumps (Dump-Dateien des kesl-Prozesses)
- /var/opt/kaspersky/kesl/common/dumps-user (Dump-Dateien der Benutzerprozesse)

Für den Zugriff auf das Standardverzeichnis zum Speichern von Dump-Dateien sind Root-Rechte erforderlich. Sie können ein anderes Verzeichnis zum Speichern der Dump-Dateien des kesl-Prozesses angeben. Wenn Sie ein anderes Verzeichnis angeben, stellen Sie sicher, dass nur root Lese- und Schreibberechtigungen für dieses Verzeichnis hat (Berechtigungen `700` oder `rwx--------`).

Für die Speicherung von Dump-Dateien benötigt das Programm Speicherplatz auf dem Datenträger zusätzlich zu dem in den Mindestanforderungen an die Hardware angegebenen Speicherplatz.

Dump-Dateien bleiben während der gesamten Nutzungsdauer des Programms auf Ihrem Computer gespeichert. Sie werden unwiderruflich gelöscht, wenn das Programm entfernt wird. Es werden keine Dump-Dateien automatisch an Kaspersky gesendet.

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:

- Ablaufverfolgung aktivieren und deaktivieren
- Stufe der Ablaufverfolgung ändern
- Protokolldateien herunterladen
- Protokoll der Remote-Installationen der Anwendung herunterladen
- Ereignisprotokolle des Systems (Syslog) herunterladen
- Anwendungen 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 der Web Console die Option **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 Link mit dem 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 Anwendung anzeigen.

So zeigen Sie das Remote-Installationsprotokoll der Anwendung 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 zur Ferndiagnose 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 Anwendung anzeigen.

So zeigen Sie das Remote-Installationsprotokoll der Anwendung 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 das Verzeichnis **Remote-Installationsprotokolle** aus.

Weitere Informationen über das Ferndiagnose-Tool finden Sie in der Hilfe zu Kaspersky Security Center.

Anwendungen

Dieser Abschnitt enthält Informationen, die den Haupttext der Hilfe ergänzen.

Anhang 1. 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:
- Vorinstallierte Konfigurationsdateien, die bei der Erstkonfiguration der Anwendung 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 Anwendungseinstellungen enthalten. Sie können diese Dateien ändern und in die Anwendung importieren, um die entsprechenden Einstellungen zu ändern.

Regeln zum Ändern von Konfigurationsdateien für die Aufgaben der Anwendung

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 Werte der Einstellungen im Format < `Einstellungsname` >=< `Einstellungswert` > an (Leerzeichen zwischen dem Einstellungsnamen und dem Einstellungswert 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.

Konfigurationsdateien für die Erstkonfiguration

Sie können die Einstellungen für die Ersteinrichtung des Programms mithilfe einer Konfigurationsdatei festlegen:

- Wenn Sie das Programm mithilfe von Kaspersky Security Center installieren, finden Sie im Archiv für die Remote-Installation des Programms die Konfigurationsdatei autoinstall.ini. Sie können Einstellungen in dieser Datei angeben, bevor Sie das Installationspaket erstellen. Kaspersky Security Center wendet diese Einstellungen während der Programminstallation an.
- Wenn Sie das Programm über die Befehlszeile installieren, müssen Sie die Konfigurationsdatei erstellen und beim Starten des Assistenten für die Ersteinrichtung den Pfad zu dieser Datei angeben. Sie können die Struktur dieser Datei aus der Konfigurationsdatei autoinstall.ini kopieren.

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. Für die Datei autoinstall.ini sind Standardwerte angegeben.

Welche Werte für einige Einstellungen gültig sind, hängt davon ab, ob Sie die Installation remote über Kaspersky Security Center oder über die Befehlszeile durchführen.

Um eine Einstellung in der Konfigurationsdatei zu ändern, geben Sie ihren Wert im Format <setting name>=<value> an.

Beispiel

```
UPDATER_SOURCE=KLServers
```

Parameter	Description	Werte

Abschnitt **[CustomSettings]**	Feinabstimmung des Programms während der Remote-Installation. Ermöglicht das Ändern einiger Einstellungen in der Datei kesl.ini sowie der Trace-Stufe.
	
	Sie können das Programm mithilfe dieses Abschnitts nur während der Erstinstallation konfigurieren.
	
	Wenn der Abschnitt `[CustomSettings]` die Einstellungen der Datei autoinstall.ini dupliziert, werden die Einstellungen von autoinstall.ini auf das Programm angewendet.
		• Beliebige Einstellung in der Konfigurationsdatei kesl.ini im Format <setting section>.<setting name>=<value>
		Beispiel
		`[CustomSettings]`
		`General.Locale=ru_RU.utf8`
		`Network.ProxyRouteTable=202`
		`Watchdog.MaxMemory=20MB`
		• `TraceLevel`, Detaillierungsgrad der Protokolldateien des Programms:
		  • `Detailed` – Detaillierte Protokolldatei des Programms erstellen.
		  • `MediumDetailed` – Protokolldatei des Programms erstellen, die Info-Meldungen und Fehlermeldungen enthält.
		  • `NotDetailed` – Protokolldatei des Programms erstellen, die Fehlermeldungen enthält.
		  • `None` (Standardwert) – Keine Protokolldatei des Programms erstellen.
		• `WdTraceLevel`, Detaillierungsgrad der Protokolldateien des Watchdog-Servers:
		  • `Detailed`, um eine detaillierte Protokolldatei des Watchdog-Servers zu erstellen.
		  • `MediumDetailed`, um eine Protokolldatei des Watchdog-Servers zu erstellen, die Info-Meldungen und Fehlermeldungen enthält.
		  • `NotDetailed`, um eine Protokolldatei des Watchdog-Servers zu erstellen, die Fehlermeldungen enthält.
		  • `None`, um keine Protokolldatei des Watchdog-Servers zu erstellen.
		  • `Product` (Standardwert), um den Wert auf den Wert `TraceLevel` festzulegen.

EULA_AGREED	Erforderliche Einstellung. Zustimmung zu den Bedingungen des Endbenutzer-Lizenzvertrags.	`Yes` (Standardwert) – Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren. `No` – Bedingungen des Endbenutzer-Lizenzvertrags nicht akzeptieren. Die Installation der App wird abgebrochen.

Parameter	Description	Werte
PRIVACY_POLICY_AGREED	Erforderliche Einstellung. Zustimmung zu den Bedingungen der Datenschutzrichtlinie.	`Yes` (Standardwert) – Bedingungen der Datenschutzrichtlinie akzeptieren. `No` – Bedingungen der Datenschutzrichtlinie nicht akzeptieren. Die Installation der App wird abgebrochen.
USE_KSN	Erforderliche Einstellung. Aktivierung der Nutzung von Kaspersky Security Network: Um die Nutzung von KSN zu aktivieren, müssen die Bedingungen der Erklärung zu Kaspersky Security Network akzeptiert werden. Wenn Kaspersky Endpoint Security im Standard-Modus verwendet wird und Sie die Verwendung von KSN aktiviert haben, wird der Cloud-Modus des Programms automatisch aktiviert. In diesem Modus verwendet Kaspersky Endpoint Security eine schlankere Version der Malware-Datenbanken.	`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. Das Ablehnen der Erklärung zu Kaspersky Security Network führt nicht zu einem Abbruch der Installation.
LOCALE	Gebietsschema, das für die Lokalisierung von Ereignissen in der App verwendet wird, die an Kaspersky Security Center gesendet werden. Zur Darstellung der grafischen Oberfläche und der Befehlszeile der Anwendung wird die Lokalisierung verwendet, die in der Umgebungsvariablen `LANG` angegeben ist. Wenn die angegebene Lokalisierung von der Anwendung nicht unterstützt wird, verwendet die Anwendung die englische Lokalisierung.	Das Gebietsschema wird im Format des RFC 3066-Standards angegeben. Mögliche Werte: • `de_DE.UTF-8` – Deutsch • `en_US.UTF-8` – Englisch (USA) • `es_MX.UTF-8` – Spanisch (Mexiko) • `fr_FR.UTF-8` – Französisch • `ja_JP.UTF-8` – Japanisch • `pt_BR.UTF-8` – Portugiesisch (Brasilien) • `ru_RU.UTF-8` – Russisch • `zh_TW.UTF-8` – Chinesisch traditionell • `zh_CN.UTF-8` – Chinesisch vereinfacht Wenn die Einstellung `LOCALE` nicht angegeben ist, wird der Sprachstandard des Betriebssystems verwendet. Wenn die Anwendung die Sprache des Betriebssystems nicht erkennt oder dessen Lokalisierung nicht unterstützt, wird Englisch (en_US.UTF-8 im Format des RFC 3066-Standards) zum Lokalisieren von Ereignissen verwendet.

Parameter	Description	Werte
INSTALL_LICENSE	In der Konfigurationsdatei autoinstall.ini: der Aktivierungscode zum Hinzufügen eines Lizenzschlüssels zum Programm. In der Konfigurationsdatei für die Befehlszeile können Sie auch den Pfad zur Schlüsseldatei angeben, um dem Programm einen Lizenzschlüssel hinzuzufügen. Die Einstellung wird nur angewendet, wenn die Anwendung im Standard-Modus verwendet wird.	`<activation code>`, wenn Sie das Programm bei der Installation über Kaspersky Security Center oder über die Befehlszeile mithilfe eines Aktivierungscodes aktivieren möchten. `<full path to key file>`, wenn Sie das Programm während der Installation über die Befehlszeile mithilfe einer Schlüsseldatei aktivieren möchten. `None` – Wenn die Anwendung während der Installation nicht aktiviert werden muss, etwa bei einer Installation in einem geschlossenen Netzwerksegment ohne Internetzugang.
UPDATER_SOURCE	Quelle für Updates der Datenbanken und Module der Anwendung aus. Dieser Parameter gilt nur, wenn die App im Standard-Modus oder im EDR-Agent-Modus verwendet wird.	`SCServer` – Administrationsserver von Kaspersky Security Center als Update-Quelle verwenden `KLServers` (Standard) – Kaspersky-Server als Update-Quelle verwenden. `<update source address>` als lokales Verzeichnis (z. B. /home/bases) oder als Remote-HTTP- oder HTTPS-Server (z. B. http://example.com/bases/).
PROXY_SERVER	Adresse des Proxy-Servers, der für die Internetverbindung verwendet wird Dieser Parameter gilt nur, wenn die App im Standard-Modus oder im EDR-Agent-Modus verwendet wird.	Adresse des Proxyservers in einem der folgenden Formate: • `[<connection protocol>://] <address of the proxy server>:<port>`, wenn für die Verbindung mit dem Proxyserver keine Authentifizierung erforderlich ist; • `[<connection protocol>://] [<user name>: [<password>]@]<address of the proxy server>:<port>`, wenn für die Verbindung mit dem Proxyserver eine Authentifizierung erforderlich ist. Geben Sie eine IPv6-Adresse in eckigen Klammern ein. Das Herstellen einer Verbindung mit dem Proxyserver über das HTTPS-Protokoll wird nicht unterstützt.
UPDATE_EXECUTE	Aufgabe zum Update der Anwendungsdatenbanken während des Erstkonfiguration starten Dieser Parameter gilt nur, wenn die App im Standard-Modus oder im EDR-Agent-Modus verwendet wird.	`Yes` (Standardwert) – Update-Aufgabe starten. `No` – Update-Aufgabe nicht starten.

Parameter	Description	Werte
KERNEL_SRCS_INSTALL	Kernel-Modul beim Starten des Schutzes vor bedrohlichen Dateien automatisch kompilieren. Dieser Parameter gilt nur für Betriebssysteme, von denen die fanotify-Technologie nicht unterstützt wird.	`Yes` (Standardwert) – Kernel-Modul beim Start des Schutzes vor bedrohlichen Dateien kompilieren. `No` – Kernel-Modul nicht kompilieren.
USE_GUI	Grafische Oberfläche der Anwendung installieren und verwenden. Dieser Parameter wird nur angewendet, wenn das Programm im Standard-Modus oder im EDR-Agent-Modus verwendet wird.	`Yes` – Grafische Oberfläche der Anwendung installieren und verwenden (die Dateien zur Installation der grafischen Oberfläche sind im Installationspaket enthalten). `No` (standardwert) – grafische Oberfläche nicht verwenden.
GROUP_CLEAN	Erforderliche Einstellung. Automatisches Entfernen von Benutzern aus den privilegierten Gruppen "kesladmin" und "keslaudit" vor der Installation der Anwendung.	`Yes` – Die Benutzer aus privilegierten Gruppen entfernen. Wenn der Wert `Yes` angegeben wurde und die Gruppe "nogroup" nicht vorhanden ist, wird die Installation unterbrochen und Sie werden aufgefordert, die Benutzer manuell aus den privilegierten Gruppen zu entfernen. `No` (Standard) – Benutzer nicht aus den privilegierten Gruppen entfernen.
ADMIN_USER	Benutzer, dem die Administratorrolle (admin) zugewiesen ist. Mit der Administratorrolle können Sie ohne Verwendung des Befehls `sudo` die Anwendungs- und Aufgabeneinstellungen über die grafische Oberfläche und die Befehlszeile der Anwendung verwalten.	
CONFIGURE_SELINUX	Automatische Konfiguration von SELinux für die Arbeit mit der Anwendung Kaspersky Endpoint Security.	`Yes` (Standardwert) – Automatische Konfiguration von SELinux für die Arbeit mit Kaspersky Endpoint Security ausführen. `No` – keine automatische SELinux-Konfiguration durchführen.

Parameter	Description	Werte
DISABLE_PROTECTION	Deaktivieren funktionaler Komponenten der Anwendung nach deren Installation. Eine Installation mit deaktivierten Komponenten kann hilfreich sein, um beispielsweise ein Problem mit der Anwendung zu reproduzieren und eine Protokolldatei zu erstellen. Wenn Sie nach der Installation der Anwendung mit dem Parameter `DISABLE_PROTECTION=Yes` die erforderlichen Komponenten aktivieren, werden die aktivierten Komponenten nach einem Neustart der Anwendung ausgeführt.	`Yes` – Schutzkomponenten und Untersuchungsaufgaben beim Start der App nach deren Installation deaktivieren. `No` – Schutzkomponenten und Untersuchungsaufgaben beim Start der App nach deren Installation nicht deaktivieren.
ENDPOINT_AGENT_MODE	Verwendung von Kaspersky Endpoint Security im EDR-Agent-Modus. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`Yes` – Kaspersky Endpoint Security wird im EDR-Agent-Modus zur Unterstützung von Kaspersky Detection and Response-Lösungen verwendet, die auf geschützten Geräten mit Antiviren-Lösungen von Drittanbietern zusammenarbeiten. `No` (Standardwert) – Kaspersky Endpoint Security wird im Standard-Modus oder im Light Agent-Modus verwendet (siehe auch Parameter "KSVLA_MODE").
EDR_EXPERT_CLOUD_MODE	Wählen Sie den Modus der Komponente Endpoint Detection and Response Expert aus. Die Einstellung wird nur angewendet, wenn die Anwendung im Standard-Modus verwendet wird. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`Yes` bedeutet, dass das Programm die Integration von Kaspersky Endpoint Detection and Response Expert (cloud) verwendet. `No` (Standardwert) bedeutet, dass das Programm die Integration in Kaspersky Endpoint Detection and Response Expert (on-premise) verwendet.
KSVLA_MODE	Verwendung von Kaspersky Endpoint Security im Light Agent-Modus. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`Yes` – Kaspersky Endpoint Security wird im Light Agent-Modus verwendet (als Teil von Kaspersky Hybrid Cloud Security for Virtualization Light Agent). `No` (Standardwert) – Kaspersky Endpoint Security wird im Standard-Modus oder im EDR-Agent-Modus verwendet (siehe Einstellung ENDPOINT_AGENT_MODE).

Parameter	Description	Werte
SERVER_MODE	Die Rolle der geschützten virtuellen Maschine (Server oder Workstation). Die Einstellung wird nur angewendet, wenn die Anwendung im Light Agent-Modus verwendet wird. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`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 Anwendung im Light Agent-Modus verwendet wird. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`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.
INTERCEPTOR_MODE	Der von Kaspersky Endpoint Security verwendete Mechanismus zum Abfangen von Systemereignissen: Der Parameter wird nur auf Geräten angewendet, deren Betriebssystem die fanotify-Technologie unterstützt. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`UseFanotify` (Standardwert) – fanotify-Technologie zum Abfangen von Systemereignissen verwenden. `UseUpdatableKernelModule` – Aktualisierbares Kernel-Modul zum Abfangen von Systemereignissen verwenden.

Parameter	Description	Werte
INTERCEPTOR_FALLBACK_STRATEGY	Von der Anwendung ausgeführte Aktion, wenn der Start des aktualisierbaren Kernel-Moduls fehlschlägt. Der Parameter wird nur auf Geräten angewendet, deren Betriebssystem die fanotify-Technologie unterstützt. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`FallbackToFanotify` (Standardwert) – Zur Verwendung der fanotify-Technologie zum Abfangen von Systemereignissen übergehen. `FallbackToLimitedMode` – Systemereignisse nicht abfangen. Bei dieser Option findet keine Dateiuntersuchung in Echtzeit statt. Dies reduziert das Schutzniveau des Geräts.
INTERCEPTOR_APPLY_STRATEGY	Wenn die Anwendung zur Verwendung des aktualisierbaren Kernel-Moduls übergeht, ist zum Starten des Moduls ein Neustart der Anwendung erforderlich. Dieser Parameter gibt an, ob die Anwendung automatisch neu gestartet wird, oder ob ein manueller Neustart der Anwendung erforderlich ist. Diese Einstellung gilt nur bei der Installation über Kaspersky Security Center. Der Parameter wird nur auf Geräten angewendet, deren Betriebssystem die fanotify-Technologie unterstützt. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`RestartServiceAutomatically` (Standardwert) – Anwendung automatisch neu starten, um das aktualisierbare Kernel-Modul zu starten. `RestartServiceManually` – Aktualisierbares Kernel-Modul starten, nachdem ein manueller Anwendungsneustart durch den Benutzer erfolgt ist. Es wird empfohlen, die Anwendung beim Übergang zur Verwendung des aktualisierbaren Kernel-Moduls automatisch neuzustarten. Nach einem manuellen Neustart kann der Start des aktualisierbaren Kernel-Moduls zu Ausführungsfehlern der Anwendung führen.
ENABLE_TRACES_ON_FIRST_STARTUP	Erstellt beim ersten Start nach der Installation eine Protokolldatei der Anwendung. Für die Protokollierung wird die Datei "kesl_startup.log" automatisch im Verzeichnis "/var/log/kaspersky/kesl/" angelegt. Für diese Datei gilt keine Größenbeschränkung, wie sie für die regulären Protokolldateien der Anwendung festgelegt sind. Die Aufzeichnung der Protokolldatei endet, sobald die Aufgabe "Schutz vor bedrohlichen Dateien" gestartet wird, oder fünf Minuten nach dem Start der Protokollierung.	`Yes` – Erstellt die Protokolldatei beim ersten Start der Anwendung nach der Installation. `No` (Standardwert) – Beim ersten Start des Programms keine Protokolldatei erstellen.

Parameter	Description	Werte
AK_FORCED_PACKAGE_MANAGER_OPERATIONS_AS_FALLBACK	Installationsmodus des Programms verwenden, der Fehler des Paketmanagers ignoriert. Dieser Modus kann verwendet werden, wenn das Programm nicht auf normale Weise installiert werden konnte. Diese Einstellung gilt nur bei der Installation über Kaspersky Security Center. Es wird empfohlen, die Änderung der Standardwerte unter Anleitung von Spezialisten des Technischen Supports vorzunehmen.	`No` (Standardwert), um das Programm normal zu installieren. `Yes`, um das Programm unter Ignorieren von Systemfehlern zu installieren.
AK_REMOVE_PARTIALLY_INSTALLED_PACKAGE	Installationspaket des Programms automatisch entfernen, wenn es nur teilweise installiert wurde. Deaktivieren Sie diese Einstellung, wenn das Programm nicht normal installiert werden konnte. Diese Einstellung gilt nur bei der Installation über Kaspersky Security Center. Es wird empfohlen, die Änderung der Standardwerte unter Anleitung von Spezialisten des Technischen Supports vorzunehmen.	`Yes` (Standardwert), um ein teilweise installiertes Installationspaket des Programms zu entfernen. `No`, um das Programm unter Ignorieren des teilweise installierten Pakets zu installieren.
AK_PACKAGE_MANAGER_DEBUG_LOG_OUTPUT	Debug-Protokolle für Paketmanager aktivieren. Diese Einstellung kann verwendet werden, wenn die App nicht ordnungsgemäß installiert werden konnte. Diese Einstellung gilt nur bei der Installation über Kaspersky Security Center. Es wird empfohlen, die Änderung der Standardwerte unter Anleitung von Spezialisten des Technischen Supports vorzunehmen.	`Yes`, um Debug-Protokolle für Paketmanager zu aktivieren. `No` (Standardwert), um Debug-Protokolle für Paketmanager nicht zu aktivieren.

Einstellungen für die Erstkonfiguration im Installationspaket

Sie können die Erstkonfigurationseinstellungen für die App im Installationspaket angeben, das Sie zur Installation der App über Kaspersky Security Center verwenden.

In der Kaspersky Security Center Web Console können Sie Parameter für die Erstkonfiguration von Kaspersky Endpoint Security in den Eigenschaften des Installationspakets auf der Registerkarte **Einstellungen** angeben. Die erstellten Installationspakete sind im Hauptfenster der Web Console in einem der folgenden Abschnitte verfügbar:

- **Entdeckung und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete**.
- **Vorgänge → Datenverwaltung → Installationspakete**.

In der Verwaltungskonsole von Kaspersky Security Center können Sie die Parameter für die Erstkonfiguration von Kaspersky Endpoint Security sowohl beim Erstellen eines Installationspakets als auch in den Eigenschaften des Installationspakets im Abschnitt **Einstellungen** angeben. Die erstellten Installationspakete sind im Strukturbaum der Verwaltungskonsole im Ordner **Erweitert → Remote-Installation → Installationspakete** verfügbar.

Der Umfang der anwendbaren Einstellungen, hängt dabei vom Nutzungsmodus der App ab.

Einstellungen für die Erstkonfiguration in der Web Console

Parameter für die Erstkonfiguration der Anwendung

Parameter	Description
Verwendungsmodus	• **Standard-Modus zum Schutz von Workstations und Servern** (Standardwert). Wenn diese Option ausgewählt ist, wird die Anwendung als autonome Anwendung zum Schutz von Workstations und Servern mit Linux-Betriebssystemen verwendet. • **Endpoint Detection and Response Agent**. Wenn diese Option gewählt ist, wird die Anwendung zusammen mit den Detection and Response-Lösungen von Kaspersky und den Anti-Virus-Lösungen von Drittanbietern auf den geschützten Maschinen eingesetzt. • **Light Agent zum Schutz virtueller Umgebungen**. Wenn diese Option ausgewählt ist, wird die App im Light Agent-Modus verwendet (als Teil von Kaspersky Security for Virtualization Light Agent). Der EDR-Agent-Modus und der Light Agent-Modus sind für Geräte mit einer Elbrus-CPU nicht verfügbar.
Endpoint Detection and Response Expert (Cloud) aktivieren	Aktivieren Sie das Kontrollkästchen, um die Integration mit Endpoint Detection and Response Expert (cloud) zu verwenden. Im Standard-Modus unterstützt die App die Integration mit Endpoint Detection and Response Expert (cloud) und Endpoint Detection and Response Expert (on-premise). Wenn dieses Kontrollkästchen deaktiviert ist, wird die Integration mit Endpoint Detection and Response Expert (on-premise) verwendet. Diese Einstellung gilt nur, wenn die App im Standard-Modus verwendet wird Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.

Parameter	Description
VDI-Schutzmodus aktivieren	Aktivieren Sie das Kontrollkästchen, um den Modus zum Schutz der VDI-Infrastruktur zu aktivieren. Dies wird empfohlen, wenn die Anwendung auf einer Vorlage für virtuelle Maschinen installiert wird, aus der temporäre virtuelle Maschinen erstellt werden. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Die Einstellung wird nur angewendet, wenn die Anwendung im Light Agent-Modus verwendet wird. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.
Die geschützte virtuelle Maschine wird als Server verwendet	Die Rolle der virtuellen Maschine, auf der die Anwendung installiert wird: Server oder Workstation. Das Kontrollkästchen ist standardmäßig aktiviert (die VM wird in der virtuellen Infrastruktur als Server verwendet). Die Einstellung wird nur angewendet, wenn die Anwendung im Light Agent-Modus verwendet wird. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.
Sprache für Ereignisse in KSC	Sprache für die Lokalisierung von App-Ereignissen, die an Kaspersky Security Center gesendet werden: • **System** (Standardwert) – zur Verwendung der Lokalisierungssprache des Betriebssystems. Wenn die Anwendung die Sprache des Betriebssystems nicht erkennt oder dessen Lokalisierung nicht unterstützt, wird Englisch zum Lokalisieren von Ereignissen verwendet. • Eine der von Kaspersky Endpoint Security unterstützten Sprachen: Englisch (USA), Spanisch (Mexiko), Chinesisch (traditionell), Chinesisch (vereinfacht), Deutsch, Portugiesisch (Brasilien), Russisch, Französisch, Japanisch. Zur Darstellung der grafischen Oberfläche und der Befehlszeile der Anwendung wird die Lokalisierung verwendet, die in der Umgebungsvariablen `LANG` angegeben ist. Wenn die angegebene Lokalisierung von der Anwendung nicht unterstützt wird, verwendet die Anwendung die englische Lokalisierung.
Programm aktivieren	Aktivieren Sie dieses Kontrollkästchen, wenn Sie während der Installation die App aktivieren möchten. Geben Sie im neuen Feld den Aktivierungscode ein. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Die Einstellung wird nur angewendet, wenn die Anwendung im Standard-Modus verwendet wird.
Update-Quellen	Quelle für Updates der Datenbanken und Module der Anwendung aus. • **Kaspersky-Update-Server** (Standardwert). • **Kaspersky Security Center**. • **Andere Quellen im lokalen oder globalen Netzwerk**. Wenn Sie diese Option auswählen, geben Sie im neuen Feld die Adresse der Update-Quelle ein. Dieser Parameter gilt nur, wenn die App im Standard-Modus oder im EDR-Agent-Modus verwendet wird.

Parameter	Description
Datenbanken-Update-Aufgabe nach der Installation ausführen	Bei aktiviertem Kontrollkästchen wird nach der Installation der Anwendung die Aufgabe zum Aktualisieren der Datenbanken und Module der Anwendung gestartet. Dieses Kontrollkästchen ist standardmäßig aktiviert. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie dem Installationspaket zuvor heruntergeladene App-Datenbanken hinzugefügt haben. Dieser Parameter gilt nur, wenn die App im Standard-Modus oder im EDR-Agent-Modus verwendet wird.
Proxyserver-Einstellungen angeben	Aktivieren Sie dieses Kontrollkästchen, wenn Sie für den Internetzugang einen Proxyserver verwenden. Geben Sie im neuen Feld die Adresse des Proxyservers in einem der folgenden Formate ein: • `[<connection protocol>://]<address of the proxy server>:<port>`, wenn für die Verbindung mit dem Proxyserver keine Authentifizierung erforderlich ist; • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`, wenn für die Verbindung mit dem Proxyserver eine Authentifizierung erforderlich ist. Geben Sie eine IPv6-Adresse in eckigen Klammern ein. Das Herstellen einer Verbindung mit dem Proxyserver über das HTTPS-Protokoll wird nicht unterstützt. Dieser Parameter gilt nur, wenn die App im Standard-Modus oder im EDR-Agent-Modus verwendet wird.
Kernel-Quellcode installieren	Bei aktiviertem Kontrollkästchen, wird unter Betriebssystemen, von denen die fanotify-Technologie nicht unterstützt wird, beim Start des Schutzes vor bedrohlichen Dateien automatisch mit der Kompilierung des Kernel-Moduls begonnen. Dieses Kontrollkästchen ist standardmäßig aktiviert. Dieser Parameter gilt nur für Betriebssysteme, von denen die fanotify-Technologie nicht unterstützt wird. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.
Grafische Benutzeroberfläche verwenden	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die grafische Oberfläche der Anwendung installieren und verwenden möchten. Dem Installationspaket müssen Dateien für die Installation der grafischen Benutzeroberfläche hinzugefügt werden. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Dieser Parameter gilt nur, wenn die App im Standard-Modus oder im EDR-Agent-Modus verwendet wird.
Einen Benutzer mit Admin-Rolle angeben	Aktivieren Sie das Kontrollkästchen, wenn Sie einen Benutzer angeben möchten, dem die Administratorrolle (admin) zugewiesen werden soll. Mit der Administratorrolle können Sie ohne Verwendung des Befehls `sudo` die Anwendungs- und Aufgabeneinstellungen über die grafische Oberfläche und die Befehlszeile der Anwendung verwalten. Geben Sie im neuen Feld den Benutzernamen ein.
SELinux automatisch konfigurieren	Wenn dieses Kontrollkästchen aktiviert ist, wird SELinux bei der Erstkonfiguration der App automatisch für die Zusammenarbeit mit Kaspersky Endpoint Security konfiguriert. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Benutzer aus privilegierten Gruppen entfernen	Aktivieren Sie das Kontrollkästchen, um vor der Installation der Anwendung die Benutzer aus den privilegierten Gruppen "kesladmin" und "keslaudit" automatisch zu entfernen. Dieses Kontrollkästchen ist standardmäßig deaktiviert. 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.

Parameter	Description
Schutzkomponenten und Untersuchungsaufgaben beim ersten Programmstart nach der Installation deaktivieren	Aktivieren Sie das Kontrollkästchen, wenn Sie die Anwendung nach der Installation mit deaktivierten Schutzkomponenten und Untersuchungsaufgaben ausführen möchten. Eine Installation mit deaktivierten Schutzkomponenten kann hilfreich sein, um beispielsweise ein Problem mit der Anwendung 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 Anwendung fortgesetzt.
Ablaufverfolgung beim ersten Programmstart nach der Installation aktivieren	Aktivieren Sie das Kontrollkästchen, wenn beim ersten Anwendungsstart nach der Installation eine Protokolldatei erstellt werden soll. Für die Protokollierung wird die Datei "kesl_startup.log" automatisch im Verzeichnis "/var/log/kaspersky/kesl/" angelegt. Für diese Datei gilt keine Größenbeschränkung, wie sie für die regulären Protokolldateien der Anwendung festgelegt sind. Die Aufzeichnung der Protokolldatei endet, sobald die Aufgabe "Schutz vor bedrohlichen Dateien" gestartet wird, oder fünf Minuten nach dem Start der Protokollierung.
Abfangmethode	Der von der Anwendung verwendete Mechanismus zum Abfangen von Systemereignissen: • **fanotify-Technologie** (Standardwert). Wenn diese Option ausgewählt ist, verwendet das Programm die Fanotify-Technologie zum Abfangen von Systemereignissen. • **Aktualisierbares Kernel-Modul**. Bei ausgewählter Option wird während der Installation der ein aktualisierbares Kernel-Modul installiert. Die Anwendung verwendet dieses Modul, um Systemereignisse abzufangen. Der Parameter wird nur auf Geräten angewendet, deren Betriebssystem die fanotify-Technologie unterstützt. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.
Wenn aktualisierbares Kernel-Modul nicht startet	Aktion, die die App ausführt, wenn das aktualisierbare Kernel-Modul nicht gestartet werden kann: • **fanotify-Technologie verwenden** (Standardwert). Wenn diese Option ausgewählt ist, wechselt das Programm zur Fanotify-Technologie zum Abfangen von Systemereignissen. • **Abfangen von Systemereignissen deaktivieren** Wenn die App das Abfangen von Systemereignissen nicht verwendet, wird keine Echtzeituntersuchung von Dateien ausgeführt und die Schutzstufe des Geräts sinkt. Dieser Parameter ist verfügbar, wenn als Abfangmechanismus die Option **Aktualisierbares Kernel-Modul** ausgewählt ist. Der Parameter wird nur auf Geräten angewendet, deren Betriebssystem die fanotify-Technologie unterstützt. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.
Modus zur Fehlerignorierung im Paketmanager aktivieren	Aktivieren Sie dieses Kontrollkästchen, um Fehler des Paketmanagers bei der Installation der App zu ignorieren. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Diese Einstellung kann verwendet werden, wenn die App nicht ordnungsgemäß installiert werden konnte. Wir empfehlen Ihnen, diese Einstellung nur unter Anleitung des Technischen Supports zu aktivieren

Einstellungen für die Erstkonfiguration in der Verwaltungskonsole

Parameter	Description
Sprache für Ereignisse in KSC	Sprache für die Lokalisierung von App-Ereignissen, die an Kaspersky Security Center gesendet werden: • **System** (Standardwert) – zur Verwendung der Lokalisierungssprache des Betriebssystems. Wenn die Anwendung die Sprache des Betriebssystems nicht erkennt oder dessen Lokalisierung nicht unterstützt, wird Englisch zum Lokalisieren von Ereignissen verwendet. • Eine der von Kaspersky Endpoint Security unterstützten Sprachen: Englisch (USA), Spanisch (Mexiko), Chinesisch (traditionell), Chinesisch (vereinfacht), Deutsch, Portugiesisch (Brasilien), Russisch, Französisch, Japanisch. Zur Darstellung der grafischen Oberfläche und der Befehlszeile der Anwendung wird die Lokalisierung verwendet, die in der Umgebungsvariablen `LANG` angegeben ist. Wenn die angegebene Lokalisierung von der Anwendung nicht unterstützt wird, verwendet die Anwendung die englische Lokalisierung.
Aktivierungscode	Wenn Sie während der Installation die App aktivieren möchten, geben Sie den Aktivierungscode ein. Die Einstellung wird nur angewendet, wenn die Anwendung im Standard-Modus verwendet wird.
Auswahl der Update-Quellen	Durch Klicken auf die Schaltfläche **Konfigurieren** wird ein Fenster geöffnet, in dem Sie die Update-Quelle für die Datenbanken und Programm-Module auswählen können: • **Kaspersky-Update-Server** (Standardwert). • **Kaspersky Security Center**. • **Andere Quelle im lokalen oder globalen Netzwerk**. Wenn Sie diese Option auswählen, geben Sie die Adresse der Update-Quelle in das Feld **Adresse** ein. Dieser Parameter gilt nur, wenn die App im Standard-Modus oder im EDR-Agent-Modus verwendet wird.
Nach Installation die Aufgabe zum Datenbank-Update starten	Bei aktiviertem Kontrollkästchen wird nach der Installation der Anwendung die Aufgabe zum Aktualisieren der Datenbanken und Module der Anwendung gestartet. Dieses Kontrollkästchen ist standardmäßig aktiviert. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie dem Installationspaket zuvor heruntergeladene App-Datenbanken hinzugefügt haben. Dieser Parameter gilt nur, wenn die App im Standard-Modus oder im EDR-Agent-Modus verwendet wird.
Adresse des Proxyservers	Wenn Sie für den Internetzugang einen Proxyserver verwenden, geben Sie die Adresse des Proxyservers in einem der folgenden Formate ein: • `[<connection protocol>://]<address of the proxy server>:<port>`, wenn für die Verbindung mit dem Proxyserver keine Authentifizierung erforderlich ist; • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`, wenn für die Verbindung mit dem Proxyserver eine Authentifizierung erforderlich ist. Geben Sie eine IPv6-Adresse in eckigen Klammern ein. Das Herstellen einer Verbindung mit dem Proxyserver über das HTTPS-Protokoll wird nicht unterstützt. Dieser Parameter gilt nur, wenn die App im Standard-Modus oder im EDR-Agent-Modus verwendet wird.

Parameter	Description
Kernel-Sourcecode installieren	Bei aktiviertem Kontrollkästchen, wird unter Betriebssystemen, von denen die fanotify-Technologie nicht unterstützt wird, beim Start des Schutzes vor bedrohlichen Dateien automatisch mit der Kompilierung des Kernel-Moduls begonnen. Dieses Kontrollkästchen ist standardmäßig aktiviert. Dieser Parameter gilt nur für Betriebssysteme, von denen die fanotify-Technologie nicht unterstützt wird. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.
Grafische Benutzeroberfläche verwenden	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die grafische Oberfläche der Anwendung installieren und verwenden möchten. Dem Installationspaket müssen Dateien für die Installation der grafischen Benutzeroberfläche hinzugefügt werden. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Dieser Parameter gilt nur, wenn die App im Standard-Modus oder im EDR-Agent-Modus verwendet wird.
Benutzer mit Administrator-Rolle (admin)	Name des Benutzers, dem Sie die Administratorrolle zuweisen möchten. Mit der Administratorrolle können Sie ohne Verwendung des Befehls `sudo` die Anwendungs- und Aufgabeneinstellungen über die grafische Oberfläche und die Befehlszeile der Anwendung verwalten.
Auto-Konfiguration von SELinux ausführen	Wenn dieses Kontrollkästchen aktiviert ist, wird SELinux bei der Erstkonfiguration der App automatisch für die Zusammenarbeit mit Kaspersky Endpoint Security konfiguriert. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Benutzer aus privilegierten Gruppen löschen	Aktivieren Sie das Kontrollkästchen, um vor der Installation der Anwendung die Benutzer aus den privilegierten Gruppen "kesladmin" und "keslaudit" automatisch zu entfernen. Dieses Kontrollkästchen ist standardmäßig deaktiviert. 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 Anwendung nach der Installation deaktivieren	Aktivieren Sie das Kontrollkästchen, wenn Sie die Anwendung nach der Installation mit deaktivierten Schutzkomponenten und Untersuchungsaufgaben ausführen möchten. Eine Installation mit deaktivierten Schutzkomponenten kann hilfreich sein, um beispielsweise ein Problem mit der Anwendung 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 Anwendung fortgesetzt.
Protokollierung der Anwendung beim ersten Start nach der Installation aktivieren	Aktivieren Sie das Kontrollkästchen, wenn beim ersten Anwendungsstart nach der Installation eine Protokolldatei erstellt werden soll. Für die Protokollierung wird die Datei "kesl_startup.log" automatisch im Verzeichnis "/var/log/kaspersky/kesl/" angelegt. Für diese Datei gilt keine Größenbeschränkung, wie sie für die regulären Protokolldateien der Anwendung festgelegt sind. Die Aufzeichnung der Protokolldatei endet, sobald die Aufgabe "Schutz vor bedrohlichen Dateien" gestartet wird, oder fünf Minuten nach dem Start der Protokollierung.
Ausführungsmodus der Anwendung	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Ausführungsmodus der Anwendung** geöffnet. In diesem Fenster können Sie einen Modus für die App auswählen. • **Standard-Modus zum Schutz von Workstations und Servern** (Standardwert). Wenn diese Option ausgewählt ist, wird die Anwendung als autonome Anwendung zum Schutz von Workstations und Servern mit Linux-Betriebssystemen verwendet. • **Endpoint Detection and Response Agent**. Wenn diese Option gewählt ist, wird die Anwendung zusammen mit den Detection and Response-Lösungen von Kaspersky und den Anti-Virus-Lösungen von Drittanbietern auf den geschützten Maschinen eingesetzt. • **Light Agent zum Schutz virtueller Umgebungen**. Wenn diese Option ausgewählt ist, wird die App im Light Agent-Modus verwendet (als Teil von Kaspersky Security for Virtualization Light Agent). Der EDR-Agent-Modus und der Light Agent-Modus sind für Geräte mit einer Elbrus-CPU nicht verfügbar.

Parameter	Description
Endpoint Detection and Response Expert (cloud) aktivieren	Aktivieren Sie das Kontrollkästchen, um die Integration mit Endpoint Detection and Response Expert (cloud) zu verwenden. Im Standard-Modus unterstützt die App die Integration mit Endpoint Detection and Response Expert (cloud) und Endpoint Detection and Response Expert (on-premise). Wenn dieses Kontrollkästchen deaktiviert ist, wird die Integration mit Endpoint Detection and Response Expert (on-premise) verwendet. Die Einstellung wird nur angewendet, wenn die Anwendung im Standard-Modus verwendet wird. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.
Die geschützte virtuelle Maschine wird als Server verwendet	Die Rolle der virtuellen Maschine, auf der die Anwendung installiert wird: Server oder Workstation. Das Kontrollkästchen ist standardmäßig aktiviert (die VM wird in der virtuellen Infrastruktur als Server verwendet). Die Einstellung wird nur angewendet, wenn die Anwendung im Light Agent-Modus verwendet wird. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.
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 Anwendung auf einer Vorlage für virtuelle Maschinen installiert wird, aus der temporäre virtuelle Maschinen erstellt werden. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Die Einstellung wird nur angewendet, wenn die Anwendung im Light Agent-Modus verwendet wird. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.
Abfangen von Systemereignissen	Diese Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Abfangen von Systemereignissen** geöffnet. In diesem Fenster können Sie einen Modus für das Abfangen von Systemereignissen auswählen, den die App verwenden soll: • **Fanotify-Technologie** (Standardwert). Wenn diese Option ausgewählt ist, verwendet das Programm die Fanotify-Technologie zum Abfangen von Systemereignissen. • **Aktualisierbares Kernel-Modul**. Bei ausgewählter Option wird während der Installation der ein aktualisierbares Kernel-Modul installiert. Die Anwendung verwendet dieses Modul, um Systemereignisse abzufangen. Der Parameter wird nur auf Geräten angewendet, deren Betriebssystem die fanotify-Technologie unterstützt. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.

Parameter	Description
Wenn aktualisierbares Kernel-Modul nicht ausführbar (Fenster **Abfangen von Systemereignissen**)	Aktion, die die App ausführt, wenn das aktualisierbare Kernel-Modul nicht gestartet werden kann: • **fanotify-Technologie verwenden** (Standardwert). Wenn diese Option ausgewählt ist, wechselt das Programm zur Fanotify-Technologie zum Abfangen von Systemereignissen. • **Abfangen von Systemereignissen deaktivieren** Wenn die App das Abfangen von Systemereignissen nicht verwendet, wird keine Echtzeituntersuchung von Dateien ausgeführt und die Schutzstufe des Geräts sinkt. Dieser Parameter ist verfügbar, wenn als Abfangmechanismus die Option **Aktualisierbares Kernel-Modul** ausgewählt ist. Der Parameter wird nur auf Geräten angewendet, deren Betriebssystem die fanotify-Technologie unterstützt. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.
Im Paket-Manager den Modus zum Ignorieren von Fehlern aktivieren	Aktivieren Sie dieses Kontrollkästchen, um Fehler des Paketmanagers bei der Installation der App zu ignorieren. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Diese Einstellung kann verwendet werden, wenn die App nicht ordnungsgemäß installiert werden konnte. Wir empfehlen Ihnen, diese Einstellung nur unter Anleitung des Technischen Supports zu aktivieren

Vorinstallierte Konfigurationsdateien

Nach der Ersteinrichtung werden in der Anwendung 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 die Werte der Einstellungen in der Datei kesl.ini ändern.

Es wird empfohlen, die Änderung der Standardwerte unter Anleitung von Spezialisten des Technischen Supports nach den von ihnen erhaltenen Anweisungen vorzunehmen.

Um die Änderungen an der Konfigurationsdatei zu übernehmen, starten Sie Kaspersky Endpoint Security neu.

Wenn der Parameter in der Datei fehlt oder ein ungültiger Parameterwert angegeben ist, verwendet die Anwendung den Standardwert.

Einstellung	Description	Werte
Der Abschnitt **[General]** enthält die folgenden Einstellungen:		
`Locale`	Sprachstandard, für die Lokalisierung der Ereignisse verwendet wird, die von der Anwendung an Kaspersky Security Center übertragen werden. Zur Darstellung der grafischen Oberfläche und der Befehlszeile der Anwendung wird die Lokalisierung verwendet, die in der Umgebungsvariablen `LANG` angegeben ist. Wenn die angegebene Lokalisierung von der Anwendung nicht unterstützt wird, verwendet die Anwendung die englische Lokalisierung.	Das Gebietsschema wird mittels RFC 3066-Format angegeben. Wenn die Einstellung `Locale` nicht angegeben ist, wird der Sprachstandard des Betriebssystems verwendet. Wenn die Anwendung die Sprache des Betriebssystems nicht erkennt oder dessen Lokalisierung nicht unterstützt, wird Englisch (en_US.UTF-8 im Format des RFC 3066-Standards) zum Lokalisieren von Ereignissen verwendet.
`PackageType`	Format des installierten Programmpakets. Es wird nicht empfohlen, den Wert dieses Parameters manuell zu ändern. Der Wert wird während der Erstkonfiguration der Anwendung automatisch eingetragen.	`rpm` – Paket wurde im RPM-Format installiert. `deb` – Paket wurde im DEB-Format installiert.
`UseFanotify`	Verwenden der fanotify-Technologie, um Dateivorgänge abzufangen. Es wird nicht empfohlen, den Wert dieses Parameters manuell zu ändern. Diese Einstellung wird bei der Erstkonfiguration des Programms festgelegt. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`true/yes` – Die Anwendung verwendet die fanotify-Technologie, um Dateivorgänge abzufangen. `false/no` – Die fanotify-Technologie wird nicht verwendet.
`KsvlaMode`	Verwendung von Kaspersky Endpoint Security im Light Agent-Modus. Es wird nicht empfohlen, den Wert dieses Parameters manuell zu ändern. Diese Einstellung wird bei der Erstkonfiguration des Programms festgelegt. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`true/yes` bedeutet, dass das Programm im Light Agent-Modus verwendet wird. `false/no` – das Programm wird im Standard-Modus verwendet.
`EndpointAgentMode`	Verwendung von Kaspersky Endpoint Security im EDR-Agent-Modus. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`true/yes` bedeutet, dass das Programm im EDR-Agent-Modus verwendet wird. `false/no` – das Programm wird im Standard-Modus verwendet.

Einstellung	Description	Werte
`KcsMode`	Die Anwendung wird innerhalb der Lösung Kaspersky Container Security als Komponente zum Schutz vor bedrohlichen Dateien verwendet. Es wird nicht empfohlen, den Wert dieses Parameters manuell zu ändern. Dieser Parameter wird nur bei einer Verwendung von Kaspersky Container Security angewendet. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`true/yes` – Die Anwendung wird innerhalb der Lösung "Kaspersky Container Security" als Komponente zum Schutz vor bedrohlichen Dateien verwendet. `false/no` (Standard) bedeutet, dass das Programm in einem der Modi von Kaspersky Endpoint Security verwendet wird (Standard-Modus, EDR-Agent-Modus oder Light Agent-Modus).
`StartupTraces`	Aktiviert die Erstellung von Protokolldateien beim Start der Anwendung.	`true/yes` – Protokolldateien beim Start der Anwendung erstellen. `false/no` (Standardwert) – Keine Protokolldateien beim Start der Anwendung erstellen.
`RevealSensitiveInfoInTraces`	Anzeigen von Informationen in Protokolldateien, die personenbezogene Daten enthalten können (z. B. Kennwörter).	`true/yes` – Informationen anzeigen, die möglicherweise personenbezogene Daten in Protokolldateien der Anwendung enthalten. `false/no` (Standardwert) – keine Informationen anzeigen, die möglicherweise personenbezogene Daten in Protokolldateien enthalten.
`AsyncTraces`	Aktivieren der asynchronen Ablaufverfolgung, bei welcher Informationen asynchron in Ablaufverfolgungsdateien geschrieben werden.	`true/yes` – asynchrone Protokollierung aktivieren. `false/no` (Standardwert) – asynchrone Protokollierung nicht aktivieren.
`MinFreeDiskSpace`	Die minimale Größe an Festplattenspeicher, die nach dem Schreiben der Dump-Datei verbleiben soll, in Megabyte.	Standardwert: 300.
`ScanMemoryLimit`	Grenzwert für die RAM-Nutzung des Programms in Megabyte.	Standardwert: 8192. Es wird empfohlen, für den Parameter `ScanMemoryLimit` einen niedrigeren Wert als für den Parameter `MaxMemory` anzugeben, damit nicht der gesamte verfügbare Speicher für die Untersuchungsaufgaben und den Anwendungsstart verwendet wird.
`MachineId`	Eindeutige ID des Geräts des Benutzers.	Der Parameterwert wird während der App-Installation automatisch ausgefüllt.
`SocketPath`	Der Pfad zum Socket für die Remote-Verbindung, der beispielsweise die GUI und das Tool kesl-control verbindet.	Standardwert: /var/run/bl4control.
`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. Wenn der Parameterwert im Betriebssystem kleiner als der Wert des Parameters `MaxInotifyWatches` ist, ändert die Anwendung den Wert des Betriebssystemparameters auf den des Parameters `MaxInotifyWatches`.	Standardwert: 299987.

Einstellung	Description	Werte
`MaxInotifyInstances`	Begrenzung der Anzahl der Einträge von Datei- und Verzeichnisänderungen pro Benutzer, die in der Datei /proc/sys/fs/inotify/max_user_instances angegeben sind. Wenn der Parameterwert im Betriebssystem kleiner als der Wert des Parameters `MaxInotifyInstances` ist, ändert die Anwendung den Wert des Betriebssystemparameters auf den des Parameters `MaxInotifyInstances`.	Standardwert: 4047.
`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: 20.
`AdditionalDNSLookup`	Verwendung von öffentlichem DNS. Wenn der Zugriff auf Server über das System-DNS fehlschlägt, verwendet die Anwendung 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: 1. Google Public DNS™ (8.8.8.8). 2. Cloudflare® DNS (1.1.1.1). 3. Alibaba Cloud® DNS (223.6.6.6). 4. Quad9® DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168).	`true/yes` – Öffentliches DNS für den Zugriff auf Kaspersky-Server verwenden. `false/no` (Standardwert) – Kein öffentliches DNS für den Zugriff auf Kaspersky-Server verwenden. Anfragen der Anwendung können Domänenadressen und die externe IP-Adresse des Benutzers enthalten, da die Anwendung eine TCP/UDP-Verbindung mit einem DNS-Server herstellt. Diese Daten sind beispielsweise erforderlich, um die Zertifikate von Webressourcen bei Zugriff über HTTPS zu überprüfen. Wenn die Anwendung einen öffentlichen DNS-Server verwendet, werden die Datenverarbeitungsregeln durch die Datenschutzrichtlinie dieses Dienstes geregelt.
`PanicThreshold`	Maximale Anzahl der Anwendungsabstürze bei Verwendung des aktualisierbaren Kernelmoduls. Beim Erreichen des angegebenen Werts wechselt die Anwendung in den "abgesicherten" Modus, in dem das aktualisierbare Kernel-Modul nicht gestartet wird. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	Standardwert: 3.
`SafeMode`	Aktivieren des „abgesicherten“ Modus bei Verwendung des aktualisierbaren Kernel-Moduls. In diesem Modus führt die Anwendung das zu aktualisierbare Kernel-Modul nicht aus. Der „abgesicherte“ Modus wird automatisch aktiviert, wenn das Programm die in der Einstellung `PanicThreshold` angegebene maximale Anzahl abnormaler Beendigungen erreicht. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`true/yes` – Der "abgesicherte" Ausführungsmodus der Anwendung ist aktiviert. `false/no` (Standardwert) – Der "abgesicherte" Ausführungsmodus der Anwendung ist deaktiviert und die Anwendung wird im normalen Modus ausgeführt.

Einstellung	Description	Werte
`GetContainerName`	Übertragen der folgenden Telemetriedaten über den Container bei einer Integration mit Kaspersky Managed Detection and Response: • Indikator dafür, dass das Ereignis in einem Container aufgetreten ist • ID des Namensraums des Containers • Name des Containers Der Name des Containers wird nur übertragen, wenn eine Lizenz für Aufgabe Untersuchung von Containern verfügbar ist und der Container eine ausreichende Lebensdauer hat. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`true/yes` (Standardwert) – Überträgt die erweiterten Telemetriedaten über den Container bei einer Integration mit Kaspersky Managed Detection and Response. `false/no` – Überträgt keine erweiterten Telemetriedaten über den Container bei einer Integration mit Kaspersky Managed Detection and Response.
`UseIncreasedXdrEventsCache`	Verwaltung des Ereignis-Caches bei Integration mit Detection and Response-Lösungen. Es besteht ein Zielkonflikt zwischen hoher Leistung und RAM-Speicherbedarf.	`true/yes` (Standardwert) minimiert die Datenträger-E/A, verwendet jedoch mehr RAM (100 MB). `false/no` verwendet weniger Arbeitsspeicher (ca. 5 MB), führt jedoch zu mehr Lese- und Schreibvorgängen auf dem Datenträger.
`FastShutdown`	Schnelles Beenden des kesl-Prozesses, wenn das Programm angehalten oder neu gestartet wird.	`true/yes` aktiviert das schnelle Beenden des kesl-Prozesses, wenn das Programm angehalten wird. `false/no` (Standardwert) deaktiviert das schnelle Beenden des kesl-Prozesses, wenn das Programm angehalten wird.
Der Abschnitt **[Network]** enthält die folgenden Einstellungen:		
`WtpFwMark`	Markierung in den Regeln des Tools "iptables", um den Datenverkehr an die Anwendung 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 Anwendungen eine andere Software ausgeführt wird, die das neunte Bit der TCP-Paketmaske verwendet, und ein Konflikt auftritt.	Der Wert wird als Dezimal- oder Hexadezimalzahl mit vorangestelltem 0x angegeben. Der Standardwert ist 0x100. Um eine zyklische Untersuchung des Datenverkehrs zu vermeiden, wenn das Programm auf Knoten ausgeführt wird, die als Teil verteilter Systeme wie Kubernetes verwendet werden, müssen Sie die Werte der Markierungen von Netzwerkpaketen mithilfe der höherwertigen Bits ändern. Zum Beispiel: 0x1000 oder 0x10000 (die Markierung ist auf eine 32-Bit-Ganzzahl beschränkt).
`NtpFwMark`	Markierung in den Regeln des Tools "iptables", um den Datenverkehr an die Anwendung umzuleiten und durch die Komponente Schutz vor Netzwerkbedrohungen zu verarbeiten. Sie müssen diese Markierung möglicherweise ändern, wenn auf demselben Gerät zusammen mit den installierten Anwendungen eine andere Software ausgeführt wird, die das neunte Bit der TCP-Paketmaske verwendet, und ein Konflikt auftritt.	Der Wert wird als Dezimal- oder Hexadezimalzahl mit vorangestelltem 0x angegeben. Der Standardwert ist 0x200. Um eine zyklische Untersuchung des Datenverkehrs zu vermeiden, wenn das Programm auf Knoten ausgeführt wird, die als Teil verteilter Systeme wie Kubernetes verwendet werden, müssen Sie die Werte der Markierungen von Netzwerkpaketen mithilfe der höherwertigen Bits ändern. Zum Beispiel: 0x2000 oder 0x20000 (die Markierung ist auf eine 32-Bit-Ganzzahl beschränkt).

Einstellung	Description	Werte
`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- oder Hexadezimalzahl mit vorangestelltem 0x angegeben. Der Standardwert ist 0x400. Um eine zyklische Untersuchung des Datenverkehrs zu vermeiden, wenn das Programm auf Knoten ausgeführt wird, die als Teil verteilter Systeme wie Kubernetes verwendet werden, müssen Sie die Werte der Markierungen von Netzwerkpaketen mithilfe der höherwertigen Bits ändern. Zum Beispiel: 0x4000 oder 0x40000 (die Markierung ist auf eine 32-Bit-Ganzzahl beschränkt).

`BypassNFlogMark`	Markierung für Pakete, die das Programm bei der Untersuchung ignoriert.	Der Wert wird als Dezimal- oder Hexadezimalzahl mit vorangestelltem 0x angegeben.
		Der Standardwert ist 0x800.
		Beispiele:
		Gesamten TCP-Datenverkehr mit dem angegebenen Gerät ignorieren:
		`iptables -t mangle -A PREROUTING -s <IP address (CIDR)> -p tcp -j MARK --set-xmark 0x800/0x800`
		`iptables -t mangle -A OUTPUT -d <IP address (CIDR)> -p tcp -j MARK --set-xmark 0x800/0x800`
		HTTPS-Server-Datenverkehr ignorieren:
		`iptables -t mangle -A PREROUTING -p tcp -m tcp --dport 443 -j MARK --set-xmark 0x800/0x800`
		`iptables -t mangle -A OUTPUT -p tcp -m tcp --sport 443 -j MARK --set-xmark 0x800/0x800`
		Um eine zyklische Untersuchung des Datenverkehrs zu vermeiden, wenn das Programm auf Knoten ausgeführt wird, die als Teil verteilter Systeme wie Kubernetes verwendet werden, müssen Sie die Werte der Markierungen von Netzwerkpaketen mithilfe der höherwertigen Bits ändern. Zum Beispiel: 0x8000 oder 0x80000 (die Markierung ist auf eine 32-Bit-Ganzzahl beschränkt).

`ProxyRouteTable`	Routing-Tabellennummer.	Standardwert: 101.
Der Abschnitt **[ScannerImpactStats]** enthält folgende Einstellungen:		
`CollectFileScanStatistics`	Aktiviert das Zählen der Statistiken zur Untersuchung von Dateien und Prozessen der Anwendung.	`true/yes` (Standardwert) – Berechnung von Statistiken zur Untersuchung von Dateien und Prozessen aktivieren. `false/no` – Berechnung von Statistiken zur Untersuchung von Dateien und Prozessen nicht aktivieren.
`StatCollectionPeriod`	Zeitintervall, in dem die Anwendung die Statistiken der untersuchten Dateien und erkannten Prozesse zählt, bevor sie in der Protokolldatei und in Berichte gespeichert werden.	Standardwert: 10 Minuten.
`StatCollectionCount`	Anzahl der untersuchten Dateien und erkannten Prozesse, die von der Anwendung in dem Zeitintervall gezählt wurden, das durch den Parameter `StatCollectionPeriod` festgelegt wird, und die in Berichte und Protokolldateien eingehen.	Standardwert: 10.
`ReportStatAmount`	Anzahl der Einträge, die in Berichten über die am häufigsten untersuchten Dateien und Prozesse pro Tag angezeigt werden.	Standardwert: 20.
Der Abschnitt **[Virtualization]** enthält die folgenden Einstellungen:		

Einstellung	Description	Werte
`ServerMode`	Rolle der geschützten virtuellen Maschine, auf der Kaspersky Endpoint Security im Light Agent-Modus verwendet wird: Server oder Workstation. Es wird nicht empfohlen, den Wert dieses Parameters manuell zu ändern. Diese Einstellung wird bei der Erstkonfiguration des Programms festgelegt. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`true/yes` – Die virtuelle Maschine wird als Server verwendet. `false/no` – Die virtuelle Maschine wird als Workstation verwendet.
`VdiMode`	Aktiviert den VDI-Schutzmodus bei Verwendung des Programms im Light Agent-Modus. Es wird nicht empfohlen, den Wert dieses Parameters manuell zu ändern. Diese Einstellung wird bei der Erstkonfiguration des Programms festgelegt. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`true/yes` – Modus zum Schutz der VDI-Infrastruktur ist aktiviert. `false/no` – Modus zum Schutz der VDI-Infrastruktur ist 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 Minuten.
`StartupTimeout`	Die maximale Wartezeit für den Start der Anwendung (in Minuten), nach dem der Watchdog-Server einen Neustart des Prozesses "kesl" durchführt.	Standardwert: 3 Minuten.
`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 Anwendung versucht, als Antwort auf eine empfangene PING-Nachricht eine PONG-Nachricht an den Watchdog-Server zuzustellen.	Standardwert: 2.000 Millisekunden.
`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 zum Neustarten des Prozesses "kesl".	Standardwert: 2 Minuten.

Einstellung	Description	Werte
`ConnectTimeout`	Maximale Wartezeit für die Verbindung der Anwendung mit dem Watchdog-Server ab dem Startzeitpunkt des Prozesses "kesl". Wenn es der Anwendung innerhalb dieses Zeitintervalls nicht gelingt, eine Verbindung herzustellen, startet der Watchdog-Server den Vorgang zum Neustarten des Prozesses "kesl".	Standardwert: 3 Minuten.
`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 Millisekunden.
`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 Minuten.
`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 Neustarten des Prozesses "kesl".	`off` – Die Nutzung des residenten Speichers ist nicht beschränkt. `<value>%` – ein Wert zwischen 1 und 100 Prozent des Arbeitsspeichers. `<value>MB` – ein Wert in Megabyte. `lowest/<value>%/<value>MB` – der kleinere Wert aus Prozentwert und absolutem Wert in Megabyte. `highest/<value>%/<value>MB` – der größere Wert aus Prozentwert und absolutem Wert in Megabyte. `auto` – bis zu 50% des verfügbaren Speichers, jedoch minimal 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 Neustarten des Prozesses "kesl".	`off` (Standardwert) – Die Nutzung des virtuellen Speichers ist unbegrenzt. `<value>MB` – ein Wert in Megabyte.
`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 Neustarten des Prozesses "kesl".	`off` (Standardwert) – Die Größe der Auslagerungsdatei ist nicht begrenzt. `<value>%` – ein Wert zwischen 0 und 100 Prozent des Arbeitsspeichers. `<value>MB` – ein Wert in Megabyte. `lowest/<value>%/<value>MB` – der kleinere Wert aus Prozentwert und absolutem Wert in Megabyte. `highest/<value>%/<value>MB` – der größere Wert aus Prozentwert und absolutem Wert in Megabyte.
`TrackProductCrashes`	Aktiviert bei Instabilität der Anwendung das Übertragen des Gerätestatus von Kaspersky Endpoint Security an Kaspersky Security Center.	`true/yes` – Aktiviert das Senden des Gerätestatus von Kaspersky Endpoint Security an Kaspersky Security Center. `false/no` (Standardwert) – Deaktiviert das Senden des Gerätestatus von Kaspersky Endpoint Security an Kaspersky Security Center.
`ProductHealthLogFile`	Pfad zu der Datei, die zur Überwachung der Anwendungsstabilität verwendet wird.	Standardwert: /var/opt/kaspersky/kesl/private/kesl_health.log
`WarnThreshold`	Zeitintervall (in Sekunden), in dem die App die Anzahl der ungeplanten Unterbrechungen zählen soll, bevor eine Warnung über Instabilität angezeigt wird.	Standardwert: 3600 Sekunden

Einstellung	Description	Werte
`WarnAfter_#_crash`	Die maximale Anzahl der Anwendungsabstürze, bei deren Erreichen eine Benachrichtigung über die instabile Anwendungsausführung angezeigt wird.	Standardwert: 10. Wenn der Wert auf 0 gesetzt ist, wird die keine Benachrichtigung über die Instabilität der Anwendung angezeigt.
`WarnRemovingThreshold`	Zeitintervall (in Sekunden), nach dem der Status "Instabil" der App entfernt wird.	Standardwert: 86400 Sekunden
`SyscallHangProbePeriod`	Die Häufigkeit, mit welcher der Watchdog-Server die Systemfunktionen "open" und "execve" aufruft und die Zähler für erfolgreiche Aufrufe dieser Funktionen erhöht.	Standardwert: 3 Sekunden
`SyscallHangCheckPeriod`	Die Häufigkeit, mit welcher der Watchdog-Server die Zähler für die erfolgreichen Aufrufe der Funktionen "open" und "execve" überprüft. Wenn sich der Wert der Zähler nach dieser Zeit nicht geändert hat, beginnt der Watchdog-Server mit dem Neustart des Prozesses "kesl".	Standardwert: 32 Sekunden
`DumpSuspendPeriod`	Die maximale Wartezeit auf den Abschluss der Erstellung einer Dump-Datei der Anwendung, für die der Watchdog-Server die Überprüfung der Anwendungsaktivität pausiert. Wenn die Erstellung der Dump-Datei nach dieser Zeit nicht abgeschlossen ist, beginnt der Watchdog-Server mit dem Neustart des Prozesses "kesl".	Mögliche Werte: 1 – 30 Minuten. Standardwert: 2 Minuten.
`TimeoutAfterCoredump`	Maximales zeitliches Intervall, in dem der Watchdog-Server nach dem Senden des SIGTRAP-Signals (das im Falle einer außerplanmäßigen Prozessbeendigung gesendet wird) das Senden weiterer Signale zum Prozess "kesl" aussetzt.	Standardwert: 2 Minuten. Es wird empfohlen, für den Parameter `TimeoutAfterCoredump` einen Wert anzugeben, der gleich oder größer ist als der Wert des Parameters `DumpSuspendPeriod`. Sie können den Wert in folgenden Maßeinheiten angeben: • `<n> day|days|d` für Tage • `<n> hour|hours|hr|h` für Stunden • `<n> minute|minutes|min|m` für Minuten • `<n> second|seconds|sec|s` für Sekunden • `<n> [msec|ms]` für Millisekunden Wenn keine Maßeinheit angegeben ist, verwendet die Anwendung automatisch den Wert in Millisekunden.
`TimeoutMaxCleanPeriod`	Die maximale Zeit, die dem Prozess zum Löschen der Firewall-Regeln des Betriebssystems zugewiesen wird. Wenn der Prozess innerhalb dieser Zeit seinen Abschluss nicht signalisiert, betrachtet der Watchdog-Server den Prozess als eingefroren.	Standardwert: 10 Sekunden
`TimeoutAfterClean`	Die maximale Zeit, die dem Prozess zum Löschen der Firewall-Regeln des Betriebssystems für den Abschluss zur Verfügung steht, nachdem der Watchdog-Server das SIGTERM-Signal an den Bereinigungsprozess gesendet hat.	Standardwert: 10 Sekunden
Der Abschnitt **[Environment]** ist in der Konfigurationsdatei standardmäßig nicht vorhanden.		

Einstellung	Description	Werte
`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. Diese Einstellung gilt nicht für Geräte mit einer Elbrus-CPU.	`true/yes` – Unterstützung der containerd-Umgebung für die Komponente "Container-Überwachung" aktivieren. `false/no` – Unterstützung der containerd-Umgebung für die Komponente "Container-Überwachung" nicht aktivieren.
`ReduceSWMemoryConsumption`	Begrenzung des Speicherverbrauchs durch die Komponente Verhaltensanalyse für die Verarbeitung der Ereigniswarteschlange. Das Festlegen einer Speicherbegrenzung wirkt sich negativ auf die Bedrohungserkennung aus, einschließlich der Qualität der Telemetriedaten, die im Rahmen der Integration mit Detection and Response-Lösungen übertragen werden. Es wird empfohlen, eine Begrenzung nur auf stark ausgelasteten Systemen und nach Kontaktaufnahme mit dem Technischen Support festzulegen, um spezifische Anweisungen zu erhalten, wenn es keine anderen Möglichkeiten gibt, das Problem des hohen Speicherverbrauchs zu lösen.	1 – den Speicherverbrauch durch die Komponente Verhaltensanalyse für die Verarbeitung der Ereigniswarteschlange begrenzen. 0 (Standard) – die Speichernutzung nicht begrenzen. Nach der Änderung dieser Einstellung ist ein Neustart der App erforderlich.

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

SkipDatabaseJournals=No

TimeLimit=60

SizeLimit=0

ActionOnThreat=DisinfectDeleteIfNotPossible

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

QueueScanTasks=0

ActionOnThreat=DisinfectDeleteIfNotPossible

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

QueueScanTasks=0

ActionOnThreat=DisinfectDeleteIfNotPossible

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

QueueScanTasks=No

ActionOnThreat=DisinfectDeleteIfNotPossible

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)

```
ConnectionTimeout=10

ApplicationUpdateMode=DownloadOnly

[Sources.item_0000]

Enabled=Yes

SourceType=KLServers

URL=
```

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

AllowToRequestTemporaryAccess=No

[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

ActionOnThreat=DisinfectDeleteIfNotPossible

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
```

```
QueueScanTasks=No
```

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

UseAEP=No

AEPMode=Block

UseTelemetryMonopolyMode=Yes

TelemetrySource=Default
```

Standardeinstellungen der Aufgabe Application_Control (ID:21)

```
AppControlMode=DenyList

AppControlRulesAction=ApplyRules
```

Standardeinstellungen der Aufgabe Inventory_Scan (ID:22)

```
ScanScripts=Yes

ScanBinaries=Yes

ScanAllExecutable=Yes

GoldenImageAction=DoNothing

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/usr/bin

AreaMask.item_0000=*
```

Standardeinstellungen der Aufgabe KATAEDR (ID:24)

```
Mode=EDRKATA

UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

EnableTelemetry=Yes

[Endpoints.item_0000]

Address=127.0.0.1

Port=443

[EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

[TelemetrySettings]

UseClientPinnedCertificate=No

ConnectionTimeout=10

RequestTimeout=10

OnlyTaggedEvents=No

[TelemetrySettings.Endpoints.item_#]

Address=

Port=443

[TelemetrySettings.EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes
```

```
MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15
```

Standardeinstellungen der Aufgabe Web_Control (ID:26)

```
WebControlDefaultAction=Allow

ComplaintRecipient=
```

Standardeinstellungen der Aufgabe Standalone_Sandbox (ID:29)

```
ConnectionTimeout=10

RequestTimeout=10

UseClientCertificate=No

SendingMode=AutoOnly

QuarantineFile=Yes

ScanCriticalAreas=Yes

CreateIocScanTask=Yes

QuarantineFileOnIocDetected=Yes

ScanCriticalAreasOnIocDetected=Yes

Drives=Critical

ScheduleMode=Manually

[Servers.item_0000]

Address=127.0.0.1

Port=443

[SandboxTransferSettings]

SandboxQueue=1024
```

Standardeinstellungen der Aufgabe KATANDR (ID:31)

```
UseClientPinnedCertificate=No

SynchronizationPeriod=5
```

```
ConnectionTimeout=10

RequestTimeout=10

[Endpoints.item_0000]

Address=127.0.0.1

Port=8081

[EventTransferSettings]

MaximumDataTransferTime=30

MaximumNumberOfEventsInPackage=1024

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

PingPeriod=450
```

Standardeinstellungen der Aufgabe KUMA (ID:33)

```
UseClientCertificate=No

UseTls=No

ConnectionTimeout=5

[Servers.item_0000]

Address=127.0.0.1

Port=443

Protocol=TCP

[SiemTransferSettings]

EventTransferTimeMax=30
```

Standardeinstellungen für die Aufgabe zum Schutz vor E-Mail-Bedrohungen (ID: 35)

```
CheckIncomingMessagesOnly=No

ActionOnThreat=DisinfectDeleteIfNotPossible
```

```
ScanFileArchive=Yes

ScanFileOffice=Yes

UseTimeLimit=No

TimeLimit=8

UseSizeLimit=No

SizeLimit=5

ExtensionFilter=Rename

UseAnalyzer=Yes

AnalyzerLevel=Medium

[ExtensionMasks.item_0000]

UseExtensionMask=Yes

ExtensionMask=*.txt

[ExtensionMasks.item_0001]

UseExtensionMask=Yes

ExtensionMask=*.run

[ExtensionMasks.item_0002]

UseExtensionMask=Yes

ExtensionMask=*.exe

[ExtensionMasks.item_0003]

UseExtensionMask=Yes

ExtensionMask=*.js

[ExtensionMasks.item_0004]

UseExtensionMask=Yes

ExtensionMask=*.jse

[ExtensionMasks.item_0005]

UseExtensionMask=Yes

ExtensionMask=*.msi
```

```
[ExtensionMasks.item_0006]

UseExtensionMask=Yes

ExtensionMask=*.scr

[ExtensionMasks.item_0007]

UseExtensionMask=Yes

ExtensionMask=*.vbe

[ExtensionMasks.item_0008]

UseExtensionMask=Yes

ExtensionMask=*.vbs

[ExtensionMasks.item_0009]

UseExtensionMask=Yes

ExtensionMask=*.sh
```

Standardeinstellungen für die Aufgabe zum Schutz vor BadUSB-Angriffen (ID: 37)

```
MaxAuthAttempts=5

TimeoutAfterAttempts=5

ProhibitOnScreenKeyboard=No

ProhibitBarcodeScanner=Yes
```

Standardeinstellungen der Aufgabe KATANDR (ID:31)

```
ConnectionTimeout=10

RequestTimeout=10

SynchronizationPeriod=5

UseTunnel=No

TunnelAddress=127.0.0.1

TunnelPort=443

[Endpoints.item_0000]
```

```
Address=127.0.0.1
Port=443
EnableTelemetry=Yes
[TelemetrySettings]

ConnectionTimeout=10
RequestTimeout=10
OnlyTaggedEvents=No
UseTunnel=No
TunnelAddress=127.0.0.1
TunnelPort=443
[TelemetrySettings.Endpoints.item_0000]

Address=127.0.0.1
Port=443
[TelemetrySettings.EventTransferSettings]

MaximumDataTransferTime=30
UseRequestCountLimits=Yes
MaximumNumberOfEventsInHour=3000
EventLimitExceededPercentage=15
MaximumNumberOfEventsInPackage=1024
```

Anhang 2. 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 Pfad zur Datei>`

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 Pfad zur Datei>
```

Anhang 3. Parameter für die Interaktion mit externen Diensten

Kaspersky Endpoint Security verwendet die folgenden Parameter für die Netzwerkeinstellungen und für die Verschlüsslung der Interaktion mit externen Diensten.

Parameter für die Interaktion mit externen Diensten

Netzwerkadresse und Protokoll des Dienstes	Description
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protokoll: HTTPS Port: 443	Aktivieren der Anwendung.

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
Protokoll: HTTPS
Port: 443
	Aktualisieren der Datenbanken und Module der Anwendung.

Netzwerkadresse und Protokoll des Dienstes	Description

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
Protokoll: `HTTP`
Port: `80`
	Aktualisieren der Datenbanken und Module der Anwendung.

`downloads.upd.kaspersky.com` Protokoll: `HTTPS` Port: `443`	• Aktualisieren der Datenbanken und Module der Anwendung. • Überprüfen des Zugriffs auf Kaspersky-Server. Wenn der Zugriff auf Server über das System-DNS fehlschlägt, verwendet die Anwendung das öffentliche DNS. Dies ist erforderlich, um die Anwendungsdatenbanken zu aktualisieren und das Sicherheitsniveau des Geräts aufrechtzuerhalten. Die Anwendung verwendet die folgenden öffentlichen DNS in der Reihenfolge, in der sie umgangen werden: 1. Google Public DNS (8.8.8.8) 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). Anfragen der Anwendung können Domänenadressen und die externe IP-Adresse des Benutzers enthalten, da die Anwendung eine TCP/UDP-Verbindung mit einem DNS-Server herstellt. Diese Daten sind beispielsweise erforderlich, um die Zertifikate von Webressourcen bei Zugriff über HTTPS zu überprüfen. Wenn die Anwendung einen öffentlichen DNS-Server verwendet, werden die Datenverarbeitungsregeln durch die Datenschutzrichtlinie dieses Dienstes geregelt.
`ds.kaspersky.com` Protokoll: `HTTPS` Port: `443`	Verwendung von Kaspersky Security Network

Netzwerkadresse und Protokoll des Dienstes	Description

`ksn-a-stat-geo.kaspersky-labs.com`
`ksn-file-geo.kaspersky-labs.com`
`ksn-verdict-geo.kaspersky-labs.com`
`ksn-url-geo.kaspersky-labs.com`
`ksn-a-p2p-geo.kaspersky-labs.com`
`ksn-cinfo-geo.kaspersky-labs.com`
Protokoll: `KSN`
Port: `443`, `1443`
	Verwendung von Kaspersky Security Network

`click.kaspersky.com` Protokoll: `HTTPS` Port: `443`	Folgen von Links in der Benutzeroberfläche.

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protokoll: `HTTP`
Port: `80`
	Public Key Infrastructure (PKI).
	Diese Server (crl.kaspersky.com) sind Teil der Public-Key-Infrastruktur (PKI) und werden benötigt, um die Gültigkeit der digitalen Signaturzertifikate von Kaspersky zu überprüfen. Der CRL-Server stellt eine Liste widerrufener Zertifikate bereit. Der OCSP-Dienst ermöglicht es, den Status eines bestimmten Zertifikats in Echtzeit abzufragen. Das Zusammenwirken dieser Komponenten gewährleistet die Sicherheit der Interaktion mit digitalen Zertifikaten und den Schutz vor möglichen Angriffen.

Anhang 4. Dateierweiterungen für die schnelle Untersuchung von Wechseldatenträgern

com – ausführbare Programmdatei mit einer Größe von maximal 64 KB

exe – ausführbare Datei, selbstextrahierendes Archiv;

sys – Systemdatei von Microsoft Windows;

prg – Text des Programms dBase™, Clipper oder Microsoft Visual FoxPro®, Programm des Pakets WAVmaker

bin – Binärdatei

bat – Batchdatei

cmd – Befehlsdatei für Microsoft Windows NT (entspricht einer bat-Datei für DOS), OS/2

dpl – komprimierte Bibliothek für Borland Delphi

dll – Dynamic Link Library

scr – Bildschirmschonerdatei für Microsoft Windows

cpl – Systemsteuerungsmodul (control panel) für Microsoft Windows

ocx – Microsoft OLE-Objekt (Object Linking and Embedding)

tsp – Programm, das im Timesharing-Modus arbeitet

drv – Gerätetreiber

vxd – Treiber für ein virtuelles Microsoft Windows-Gerät

pif – Datei mit Programminformationen

lnk – Linkdatei für Microsoft Windows

reg – Registrierungsschlüsseldatei für Systemregistrierung von Microsoft Windows

ini – Konfigurationsdatei, die Einstellungsdaten für Microsoft Windows, Windows NT und andere Programme enthält

cla – Java-Klasse

vbs – Visual Basic®-Skript

vbe – BIOS-Video-Erweiterung

js, jse – JavaScript-Quelltext

htm – Hypertext-Dokument

htt – Hypertext-Dokumentvorlage für Microsoft Windows

hta – Hypertext-Programm für Microsoft Internet Explorer®;

asp – Active Server Pages-Skript;

chm – kompilierte HTML-Datei

pht – HTML-Datei mit eingebetteten PHP-Skripten

php – Skript, das in eine HTML-Datei eingebettet wird

wsh – Datei für Microsoft Windows Script Host

wsf – Skript von Microsoft Windows

the – Bildschirmschonerdatei für den Arbeitsplatz von Microsoft Windows 95

hlp – Hilfedatei im Format Win Help

msg – E-Mail-Nachricht für Microsoft Mail

plg – E-Mail-Nachricht

mbx – gespeicherte E-Mail-Nachricht für Microsoft Office Outlook

doc* – Dokumente für Microsoft Office Word, z.B.: doc – Dokumente für Microsoft Office Word, docx – Dokument für Microsoft Office Word 2007 mit XML-Unterstützung, docm – Dokument für Microsoft Office Word 2007 mit Makro-Unterstützung

dot* – Dokumentvorlagen in Microsoft Office Word, z.B. dot – Dokumentvorlage in Microsoft Office Word, dotx – Dokumentvorlage in Microsoft Office Word 2007, dotm – Dokumentvorlage in Microsoft Office Word 2007 mit Makrounterstützung.

fpm – Datenbankprogramm, Startdatei für Microsoft Visual FoxPro

rtf – Rich Text Format-Dokument

shs – Datenauszug für Windows Shell Scrap Object Handler

dwg – Datenbank für AutoCAD®-Skizzen

msi – Microsoft Windows Installer-Paket

otm – VBA-Projekt für Microsoft Office Outlook.

pdf – Dokument für Adobe Acrobat

swf – Objekt für Shockwave® Flash

jpg, jpeg – komprimierte Bilddatei

emf – Enhanced Metafile

ico – Symboldatei für ein Objekt

ov? – ausführbare Dateien für Microsoft Office Word

xl* – Dokumente und Dateien für Microsoft Office Excel, z.B.: xla – Erweiterung für Microsoft Office Excel, xlc – Diagramm, xlt – Dokumentvorlage, xlsx – Arbeitsblatt für Microsoft Office Excel 2007, xltm – Arbeitsblatt für Microsoft Office Excel 2007 mit Makro-Unterstützung, xlsb – Arbeitsblatt für Microsoft Office Excel 2007 im Binärformat (nicht XML), xltx – Vorlage für Microsoft Office Excel 2007, xlsm – Vorlage für Microsoft Office Excel 2007 mit Makro-Unterstützung, xlam – Konfigurationsdatei für Microsoft Office Excel 2007 mit Makro-Unterstützung.

pp* – Dokumente und Dateien für Microsoft Office PowerPoint®, z.B.: pps – Folie für Microsoft Office PowerPoint, ppt – Präsentation, pptx – Präsentation für Microsoft Office PowerPoint 2007, pptm – Präsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, potx – Präsentationsvorlage für Microsoft Office PowerPoint 2007, potm – Präsentationsvorlage für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, ppsx – Folienpräsentation für Microsoft Office PowerPoint 2007, ppsm – Folienpräsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, ppam – Konfigurationsdatei für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung.

md* – Dokumente und Dateien für Microsoft Office Access®, z.B.: mda – Arbeitsgruppe für Microsoft Office Access, mdb – Datenbank.

sldx – Folie in Microsoft Office PowerPoint 2007

sldm – Folie in Microsoft Office PowerPoint 2007 mit Makrounterstützung

thmx – Thema in Microsoft Office 2007

Anhang 5. Variablen in Nachrichtenvorlagen

Mithilfe der Komponenten Gerätekontrolle und Web-Kontrolle können Sie Vorlagen für Nachrichten anpassen, die Kaspersky Endpoint Security einem Benutzer anzeigt, der versucht, auf ein blockiertes Gerät, ein Programm oder eine Ressource zuzugreifen oder eine potenziell gefährliche Aktion auszuführen.

Zum Erstellen von Nachrichtenvorlagen stehen spezielle Variablen zur Verfügung (z. B. `%USER_NAME%`). Wenn Sie Variablen verwenden, kann ein und dieselbe Nachrichtenvorlage für verschiedene Computer genutzt werden. Wenn eine Nachricht generiert wird, ruft Kaspersky Endpoint Security den Wert der Variablen aus den Betriebssystemeinstellungen ab und fügt ihn passend zum Computer, Benutzer und Ereignis in die Nachricht ein.

Variablen in Nachrichtenvorlagen der Gerätekontrolle

In Vorlagen für Nachrichten an Benutzer oder an den Administrator können Sie die folgenden Variablen verwenden:

- **Benutzer** – `%USER_NAME%`.

  Name des aktuellen Benutzerkontos auf dem Computer, auf dem die Nachricht erstellt wurde, im Format `<device name>\<user alias>` (z. B. `DESKTOP-123\John.Smith`).

- **Computername** – `%COMPUTER_NAME%`.

  Name des Computers, auf dem ein Gerät blockiert wurde.

- **Regelname** – `%RULE%`.

  Name der Regel, durch die ein Gerät blockiert wurde.

- **Auslösedatum der Regel** – `%DATE%`.

  Datum, an dem das Gerät blockiert wurde (im Format TT.MM.JJJJ).

- **Auslöse-Uhrzeit der Regel** – `%TIME%`.

  Uhrzeit, zu der das Gerät blockiert wurde (im Format hh:mm).

- **Gerätename** – `%DEVICE_NAME%`.

  Name des blockierten Geräts.

- **Gerätetyp** – `%DEVICE_TYPE%`.

  Typ des blockierten Geräts (z. B. Drucker, Wechseldatenträger, CD/DVD-Laufwerke).

- **Gerätemodell** – `%DEVICE_VIDPID%`.

  Modell des blockierten Geräts (z. B. VID_1234&PID_5678).

- **Geräte-ID** – `%DEVICE_ID%`.

  ID des blockierten Geräts (z. B. `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`).

- **Vorgänge mit Geräten** – `%OPERATION%`.

  Typ des verbotenen Vorgangs mit dem Gerät.

Variablen in Nachrichtenvorlagen der Web-Kontrolle

In Vorlagen für Nachrichten an Benutzer oder an den Administrator können Sie die folgenden Variablen verwenden:

- **Benutzer** – %USER_NAME%.

  Name des aktuellen Benutzerkontos auf dem Computer, auf dem die Nachricht erstellt wurde, im Format <device name>\<user alias> (z. B. DESKTOP-123\John.Smith).

- **Adresse der Webseite** – %CANONIC_REQUEST_URL%.

  Adresse der blockierten Webressource.

- **Regelname** – %RULE%.

  Name der Regel, durch die eine Webressource blockiert wurde.

- **Empfängeradresse für die Nachricht** – %COMPLAIN_EMAIL%.

  E-Mail-Adresse für das Feedback über blockierte Webressourcen. Durch Klick auf die E-Mail-Adresse wird ein Fenster geöffnet, in dem der Benutzer eine Nachricht an den Administrator schreiben kann.

- **Name der Inhaltskategorie** – %CONTENT_CATEGORY_LIST%.

  Website-Kategorie, zu der die blockierte Ressource gehört (z. B. *Zahlungssysteme*).

- **Name der Datentypkategorie** – %TYPE_CATEGORY_LIST%.

  Kategorie für den Typ der Daten, die sich auf der blockierten Webressource befinden (z. B. *Bilddateien*).

- **Link zur angeforderten Webseite** – %CONTINUE_PAGE%.

  Link zur angeforderten Webseite (z. B. http://www.example.com/pagename.html).

- **Link zur Website** – %CONTINUE_SITE%.

  Link zur Website, die die angeforderte Webseite enthält (z. B. http://www.example.com/).

- **Link für den Zugriff auf Domänen** – %CONTINUE_DOMAIN%.

  Durch Klick auf diesen Link kann auf alle vorhandenen Webseiten des Domänennamens zugegriffen werden. Beispiel: Wenn die Adresse der blockierten Webseite http://www.example.com lautet, wird die Variable %CONTINUE_DOMAIN% durch den Link http://*.example.com ersetzt. Mit diesem Link können Sie auf alle Webadressen des zugrunde liegenden Domänennamens http://www.example.com/ zugreifen, auch auf untergeordnete Domänen wie z. B. http://start.example.com/* oder http://domain.domain.example.com/*. Dabei steht das Zeichen * für eine beliebige Zeichenfolge (einschließlich einer leeren Zeichenfolge).

Anhang 6. Programmereignisse

Informationen über die Ausführung der einzelnen Komponenten von Kaspersky Endpoint Security, über Ereignisse bei der Datenverschlüsselung, über den Abschluss der einzelnen Aufgaben zur Schadsoftware-Untersuchung, der Update-Aufgabe und der Aufgabe zur Integritätsprüfung sowie über die allgemeine Programmausführung werden im Kaspersky Security Center-Ereignisprotokoll und im Ereignisprotokoll des Betriebssystems (syslog) protokolliert.

Kritisch

Verletzung der Systemintegrität

Zustand	ⓘ
Komponente	Überwachung der System-Integrität
Linux-Ereignis-ID	0
Ereignis-ID in Kaspersky Security Center	GNRL_EV_FIM_ALARM
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Anwendungsstart verweigert

Zustand	ⓘ
Komponente	Programmkontrolle
Linux-Ereignis-ID	122
Ereignis-ID in Kaspersky Security Center	GNRL_EV_APPLICATION_LAUNCH_DENIED
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Schädliches Objekt erkannt (lokale Datenbanken)

Zustand	ⓘ
Komponente	Schutz vor bedrohlichen Dateien Schutz vor E-Mail-Bedrohungen Verhaltensanalyse Exploit-Prävention Sandbox
Linux-Ereignis-ID	6
Ereignis-ID in Kaspersky Security Center	GNRL_EV_VIRUS_FOUND
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Grenzwert für Ereignisse der Überwachung der Systemintegrität überschritten

Zustand	ⓘ
Komponente	Überwachung der System-Integrität
Linux-Ereignis-ID	70
Ereignis-ID in Kaspersky Security Center	GNRL_EV_FIM_ALARM_OVERFLOW
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Vorgang mit dem Gerät verboten

Zustand	ⓘ
Komponente	Gerätekontrolle
Linux-Ereignis-ID	94
Ereignis-ID in Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Netzwerkangriff erkannt

Zustand	⊗
Komponente	Schutz vor Netzwerkbedrohungen
Linux-Ereignis-ID	102
Ereignis-ID in Kaspersky Security Center	GNRL_EV_ATTACK_DETECTED
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Zugriff verweigert (lokale Datenbanken)

Zustand	⊗
Komponente	Web-Kontrolle
Linux-Ereignis-ID	190
Ereignis-ID in Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Warnung

Desinfektion nicht möglich

Zustand	⚠
Komponente	Schutz vor bedrohlichen Dateien Schutz vor E-Mail-Bedrohungen
Linux-Ereignis-ID	10
Ereignis-ID in Kaspersky Security Center	GNRL_EV_OBJECT_NOTCURED
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Warnung vor unerwünschten Inhalten (lokale Datenbanken)

Zustand	⚠
Komponente	Web-Kontrolle
Linux-Ereignis-ID	192
Ereignis-ID in Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Nachricht an den Administrator bezüglich der Sperrung des Zugriffs auf eine Webseite

Zustand	⚠
Komponente	Web-Kontrolle
Linux-Ereignis-ID	196

Ereignis-ID in Kaspersky Security Center	GNRL_EV_WC_USER_REQUEST
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Informative Meldung

Objekt desinfiziert

Zustand	ⓘ
Komponente	Schutz vor bedrohlichen Dateien Schutz vor E-Mail-Bedrohungen
Linux-Ereignis-ID	9
Ereignis-ID in Kaspersky Security Center	GNRL_EV_OBJECT_CURED
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt gelöscht

Zustand	ⓘ
Komponente	Schutz vor bedrohlichen Dateien Schutz vor E-Mail-Bedrohungen
Linux-Ereignis-ID	8
Ereignis-ID in Kaspersky Security Center	GNRL_EV_OBJECT_DELETED
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Programmstart erlaubt

Zustand	ⓘ
Komponente	Programmkontrolle
Linux-Ereignis-ID	120
Ereignis-ID in Kaspersky Security Center	GNRL_EV_APPLICATION_LAUNCHED
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center	nicht konfiguriert

Programmstart im Testmodus erlaubt

Zustand	ⓘ
Komponente	Programmkontrolle
Linux-Ereignis-ID	121
Ereignis-ID in Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Programmstart im Testmodus verweigert

Zustand	ⓘ
Komponente	Programmkontrolle
Linux-Ereignis-ID	123
Ereignis-ID in Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_DENIED
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Gerät verbunden

Zustand	ⓘ
Komponente	Gerätekontrolle
Linux-Ereignis-ID	90
Ereignis-ID in Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUGGED
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Gerät getrennt

Zustand	ⓘ
Komponente	Gerätekontrolle
Linux-Ereignis-ID	91
Ereignis-ID in Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
Protokoll (syslog) (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Anhang 7. Rückgabecodes

Rückgabe-Codes des Assistenten für die Ersteinrichtung

0 – Die Installation wurde erfolgreich abgeschlossen.

Kritische Fehler

1 – Unbekannter Fehler (alle anderen kritischen Fehler außer den unten aufgeführten, zum Beispiel: Systemfehler, unzureichender Arbeitsspeicher, Fehler beim Öffnen von Dateien und andere).

2 – Die Konfigurationsdatei für die Ersteinrichtung enthält ungültige Parameter.

3 – Das Programm konnte nicht installiert oder aktualisiert werden.

4 – Das Programm kann nicht entfernt werden.

5 – Das Programm kann nicht gestartet werden. Mögliche Ursache: Die Zugriffsrechte sind falsch konfiguriert. Vergewissern Sie sich, dass nur das Root-Benutzerkonto Schreibrechte für die folgenden Verzeichnisse hat: /, /opt, /opt/kaspersky, /var, /var/opt, /var/opt/kaspersky, /usr und /usr/lib64.

6 – Die erforderlichen Aktionen wurden vor der Installation nicht ausgeführt.

7 – Das Programm konnte nicht aktualisiert werden. Die Installation einer früheren Version des Programms wird nicht unterstützt.

8 – Benutzer konnten nicht aus privilegierten Gruppen entfernt werden.

9 – Es konnte keine eindeutige MachineID für die Programminstallation erstellt werden.

10 – Das Programm konnte nicht gestartet oder neu gestartet werden.

11 – Die Bedingungen des Endbenutzer-Lizenzvertrags (EULA) und der Datenschutzrichtlinie wurden nicht akzeptiert.

12 – Das Programm kann nicht gleichzeitig im Light Agent-Modus und im EDR Agent-Modus verwendet werden.

13 – Das Paket astra-digsig-oldkeys für den Modus der geschlossenen Softwareumgebung in Astra Linux wurde nicht gefunden.

14 – Die Ersteinrichtung wurde bereits gestartet.

15 – Die Komponente Light Agent for Linux, die als Teil der Lösung Kaspersky Security for Virtualization 5.2 Light Agent installiert wurde, muss entfernt werden.

16 – Der Kaspersky Security Center Administrationsagent muss installiert sein.

17 – Der Assistent für die Ersteinrichtung konnte nicht gestartet werden, da bereits ein Programmprozess ausgeführt wird.

18 – fanotify wird nicht unterstützt. Ein Kernel-Modul für den Schutz vor bedrohlichen Dateien konnte nicht kompiliert werden.

19 – Für die Installation sind Administratorrechte erforderlich.

20 – Der Programmdienst wurde nicht gestartet.

21 – Das Programm-Update wurde zurückgesetzt.

22 – Die Integration des Programms im EDR Agent-Modus oder im Light Agent-Modus mit Kaspersky Endpoint Detection and Response Expert (cloud) wird nicht unterstützt.

Warnungen

71 – Mehrere Warnungen während der Installation. Ausführliche Informationen finden Sie im Installationsprotokoll.

72 – Die Programmdatenbanken konnten nicht aktualisiert werden.

75 – Ein Neustart des Betriebssystems ist erforderlich.

76 – Die KSN-Einstellungen konnten nicht übernommen werden oder die Bedingungen der KSN-Erklärung wurden nicht akzeptiert.

77 – Ein aktualisierbares Kernel-Modul konnte nicht gestartet werden.

79 – Das Paket für die grafische Benutzeroberfläche des Programms konnte nicht installiert oder aktualisiert werden.

80 – Die Programmdatenbanken konnten nicht heruntergeladen werden.

81 – Die Aktivierung des Programms wurde aufgrund von Netzwerkproblemen mit einem Fehler beendet.

82 – Das Programm wird durch eine Richtlinie verwaltet.

83 – Die grafische Benutzeroberfläche des Programms wurde nicht gestartet.

84 – Die Administratorrolle konnte nicht zugewiesen werden. Der angegebene Benutzer wurde nicht gefunden.

85 – Das Programmpaket konnte nur im fehlerignorierenden Modus des Paketmanagers installiert oder aktualisiert werden.

86 – Das Paket für die grafische Benutzeroberfläche des Programms konnte nicht entfernt werden.

87 – Das Programmpaket konnte nur im fehlerignorierenden Modus des Paketmanagers entfernt werden.

88 – Dem Benutzer konnte die Administratorrolle nicht zugewiesen werden.

89 – Ungültiger Lizenzschlüssel.

90 – Der Zeitplan für die Update-Aufgabe konnte nicht festgelegt werden.

Rückgabecodes des Befehlszeilen-Dienstprogramms kesl-control

0 – Befehl/Aufgabe erfolgreich ausgeführt.

1 – Allgemeiner Fehler in der Befehlssyntax.

2 – Fehler in den übergebenen Anwendungseinstellungen.

64 – Kaspersky Endpoint Security wird nicht ausgeführt.

66 – Programmdatenbanken sind nicht geladen (wird nur vom Befehl `kesl-control --app-info` verwendet).

67 – Die Aktivierung des Programms wurde aufgrund von Netzwerkproblemen mit einem Fehler beendet.

68 – Der Befehl kann nicht ausgeführt werden, da das Programm durch eine Richtlinie verwaltet wird.

69 – Das Programm 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 gestoppte Aufgabe zu stoppen, eine angehaltene Aufgabe anzuhalten oder eine laufende Aufgabe fortzusetzen.

71 – Erklärung zu Kaspersky Security Network nicht akzeptiert

72 – Während der Ausführung der Aufgabe zur Benutzerdefinierten Untersuchung oder Benutzerdefinierten Untersuchung von Containern wurden Bedrohungen erkannt.

73 – Versuch, die Einstellungen der Aufgabe „Programmkontrolle“, die sich auf die Ausführung des Programms auswirken, ohne Bestätigung mithilfe der Option `--accept` festzulegen.

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.

78 – Der Befehl/die Aufgabe kann nicht ausgeführt werden, da das Programm im Light Agent-Modus verwendet wird.

79 – Der Befehl kann nicht ausgeführt werden, da das Programm im Standard-Modus verwendet wird.

80 – Der Vorgang zum Herunterladen des Updates ist aufgrund von Netzwerkproblemen fehlgeschlagen.

81 – Die Komponente wird in der Version des Betriebssystems, die auf dem Gerät installiert ist, nicht unterstützt.

128 – Unbekannter Fehler.

65 – Alle übrigen Fehler

Anhang 8. Archiv mit Programmdatenbanken vorbereiten

Beim manuellen Erstellen eines Installationspakets für Kaspersky Endpoint Security können Sie diesem zuvor heruntergeladene Programmdatenbanken hinzufügen. Wenn Sie für die Installation ein Installationspaket mit integrierten Datenbanken verwenden, wird die Anwendung mit einsatzbereiten Datenbanken installiert und eine Aktualisierung der Datenbanken nach der Installation ist nicht erforderlich.

Durch das Hinzufügen von Programmdatenbanken zum Installationspaket wird das Paket größer.

Für jede Kombination aus Architektur und Bit-Version des Betriebssystems auf Ihren geschützten Geräten benötigen Sie einen separaten Satz von Programmdatenbanken. Sie können dem Installationspaket ein Archiv hinzufügen, das einen oder mehrere Sätze von Programmdatenbanken enthält. Für die Vorbereitung jedes Satzes von Programmdatenbanken benötigen Sie eine Instanz von Kaspersky Endpoint Security, die bereits auf einem Gerät mit einem Betriebssystem passender Architektur und Bit-Version installiert ist.

So bereiten Sie ein Archiv mit Datenbanken vor:

1. Installieren Sie Kaspersky Endpoint Security auf dem Gerät und führen Sie die Erstkonfiguration mithilfe von Kaspersky Security Center oder über die Befehlszeile durch.

2. Aktualisieren Sie die Programmdatenbanken auf dem Gerät. Sie können die Datenbanken während der Erstkonfiguration des Programms oder nach der Installation aktualisieren, indem Sie über die Befehlszeile eine Aufgabe vom Typ *Update* oder in Kaspersky Security Center eine Aufgabe vom Typ *Update* ausführen.

3. Erstellen Sie abhängig von der Architektur und Bit-Version des Betriebssystems auf dem geschützten Gerät ein Verzeichnis für die Datenbanken:

   - x86_64, wenn das Programm auf einem 64-Bit-Betriebssystem installiert ist
   - i386, wenn das Programm auf einem 32-Bit-Betriebssystem installiert ist
   - arm64, wenn das Programm auf einem 64-Bit-Betriebssystem für die Arm-Architektur installiert ist
   - e2k, wenn das Programm auf einem 64-Bit-Betriebssystem für die Elbrus-Architektur installiert ist

4. Kopieren Sie den Inhalt des Verzeichnisses /var/opt/kaspersky/kesl/private/updates in das erstellte Datenbankverzeichnis.

5. Fügen Sie das erstellte Datenbankverzeichnis dem Archiv kesl-bases.tgz hinzu.

   Wenn Sie ein Installationspaket für die Installation auf mehreren Betriebssystemen mit unterschiedlichen Architekturen und Bit-Versionen erstellen möchten, müssen Sie mehrere Verzeichnisse mit Datenbanken vorbereiten und alle zum Archiv kesl-bases.tgz hinzufügen.

Die Aufgabe zum Datenbanken-Update wird standardmäßig nach der Installation von Kaspersky Endpoint Security gestartet. Wenn Sie ein Programm aus einem Installationspaket mit integrierten Datenbanken installieren, deaktivieren Sie nach der Installation des Programms die Aufgabe zum Datenbanken-Update. Sie können diese Einstellung in den Eigenschaften des erstellten Installationspakets oder in der Konfigurationsdatei autoinstall.ini (`UPDATE_EXECUTE=No`) konfigurieren.

Anhang 9. Anforderungen an IOC-Dateien

Beim Erstellen von IOC-Suchaufgaben sind die folgenden Anforderungen und Einschränkungen in Bezug auf IOC-Dateien beachten:

- Die Anwendung 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 Anwendung fehlende Übereinstimmungen festgehalten.
- Die IDs aller IOC-Dateien, die innerhalb einer IOC-Suchaufgabe verwendet werden, müssen eindeutig sein. Das Vorhandensein von IOC-Dateien mit dem gleichen Identifikator kann sich auf die Ergebnisse der Aufgabenausführung auswirken.
- 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.

DIE DATEI IOC TERMS.XLSX HERUNTERLADEN

In der folgenden Tabelle sind Besonderheiten und Einschränkungen der Anwendung 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 (zulässige 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 Anwendung 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`
	  • 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 time zone, UTC` angegeben sind.

Rechtliche Hinweise

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.

Ausführliche Informationen über die Verarbeitung, Speicherung und Vernichtung von Informationen, die während der Nutzung der Anwendung erhalten und an Kaspersky übertragen werden, finden Sie im Endbenutzer-Lizenzvertrag, in der Erklärung zu Kaspersky Security Network und in 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 Anwendung.

Daten, die bei Verwendung eines Aktivierungscodes bereitgestellt werden

Wenn Kaspersky Endpoint Security im Standard-Modus oder im EDR Agent-Modus verwendet und mit einem Aktivierungscode aktiviert wird, 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 Anwendung;
- Versionen der installierten Updates für die Anwendung;
- Geräte-ID und ID der Installation der Anwendung auf dem Gerät;
- Aktivierungscode, mit dem die Anwendung aktiviert wurde;
- ID der aktuellen Lizenz;
- Datum und Uhrzeit der Erstellung des Lizenzschlüssels der Anwendung;
- Datum und Uhrzeit auf dem Benutzergerät
- Datum und Uhrzeit, zu denen die Gültigkeitsdauer der Anwendungslizenz abläuft;
- 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 oder im EDR Agent-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 bereitgestellt werden können:

- von der Lizenz abgeleitete Anwendungs-ID;
- vollständige Version der Anwendung;
- ID der Anwendungslizenz;
- Typ der verwendeten Anwendungslizenz;
- ID der Anwendungsinstallation (PCID);
- ID des Starts des Updates der Anwendung;
- Webadresse, die verarbeitet wird.

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

Wenn Kaspersky Endpoint Security im Light Agent-Modus als Teil von Kaspersky Security for Virtualization Light Agent verwendet wird, speichert die App während der Ausführung die folgenden Informationen, die personenbezogene und vertrauliche Daten enthalten können, und sendet sie an andere Komponenten der Lösung.

- 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.
- Für ein Datenbanken-Update des Light Agent 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-Auswahl 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 Anwendung an Kaspersky Security Center übertragen werden

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

- Informationen zu den in der Anwendung verwendeten Datenbanken:
    - Liste der von der Anwendung benötigten Datenbank-Kategorien
    - Zeitpunkt (Datum und Uhrzeit), zu dem die verwendeten Datenbanken veröffentlicht und in die Anwendung geladen wurden
    - Erscheinungsdatum der heruntergeladenen Updates der Anwendungsdatenbanken
    - Zeitpunkt des letzten Updates der Anwendungsdatenbanken
    - Anzahl der Einträge in den aktuell verwendeten Anwendungsdatenbanken
- 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 Anwendung mit einem Aktivierungscode aktiviert wurde
- ID der Anwendung, 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 Anwendung 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 Anwendung auf dem Gerät
- Datum und Uhrzeit des Ablaufs der Lizenz auf dem Gerät

- Informationen zu Updates der Anwendung:
  - 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 Update der Anwendung
  - ID und Text der Erklärung zu Kaspersky Security Network für das Update der Anwendung
  - 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 Updates der Anwendung, 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 Anwendung im Rahmen eines Updates der Anwendung
- 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 Anwendung und Status aller ihrer Komponenten; Informationen zur Einhaltung von Richtlinien; Status des Echtzeitschutzes des Geräts; Status der Anwendungsstabilität; Informationen über Unterbrechungen der Anwendungsausführung.

- 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 Anwendungseinstellungen

- 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 Anwendungsdatenbanken, 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 Anwendungskomponente und die Ausführung jeder Aufgabe in Form von Ereignissen:

  - Datum und Uhrzeit, an dem Ereignis aufgetreten ist

  - Name und Typ des Ereignisses

  - Ereigniskategorie

  - Name der Aufgabe oder Komponente der Anwendung, bei deren Ausführung das Ereignis eingetreten ist

  - Informationen zu der Anwendung, die ein Ereignis verursacht hat: Name der Anwendung, Pfad der Datei auf der Festplatte, Prozess-ID, Werte der Einstellungen, falls das Ereignis sich auf den Start der Anwendung oder die Änderung der Betriebseinstellungen bezieht

  - Benutzer-ID

  - Name des Initiators (Aufgabenplanung, Name der Anwendung, 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 Anwendung 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 Anwendungsdatenbanken (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)
- Anwendungseinstellungen und Netzwerkeinstellungen
- Informationen über die ausgelöste Regel für die Programmkontrolle (Name und Typ) und das Ergebnis der Anwendung dieser Regel
- 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 Anwendung verwendeten Komponente von 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 Anwendung gehört; KL-Kategorien, zu der die Anwendung gehört; Zeitpunkt, zu dem die Datei erstmals gestartet wurde; Vertrauensgruppe, zu der die Anwendung gehört; Name und Version der Anwendung; Name des Herstellers der Anwendung; Informationen zu dem Zertifikat, mit dem die Anwendung signiert ist: Seriennummer, Fingerabdruck, Herausgeber, Antragsteller, 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 in der Oberfläche der Anwendung bereitgestellt werden

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

- vollständige Version der Anwendung;
- Lokalisierung der Anwendung;
- Anwendungs-ID (PID);
- Name des Links.

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

Welche Daten Kaspersky Security Network an Kaspersky übermittelt, hängt von der Art der Nutzung von Kaspersky Security Network ab.

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

Datenbereitstellung bei Nutzung von KSN im Standard-Modus

Wenn Sie Kaspersky Security Network im standardmäßigen KSN-Modus verwenden (in der Web Console ist der Schalter **Kaspersky Security Network (KSN) verwenden** aktiviert und das Kontrollkästchen **Erweiterten KSN-Modus verwenden** deaktiviert, in der Verwaltungskonsole ist die Option **Standardmäßiger KSN-Modus** ausgewählt), stimmen Sie durch das Akzeptieren der Bedingungen der Erklärung zu Kaspersky Security Network zu, Kaspersky automatisch die folgenden Informationen bereitzustellen.

Bereitstellung von Daten bei Verwendung von KSN im erweiterten Modus

Wenn Sie Kaspersky Security Network im erweiterten KSN-Modus verwenden (in der Web Console ist der Schalter **Kaspersky Security Network (KSN) verwenden** aktiviert und das Kontrollkästchen **Erweiterten KSN-Modus verwenden** ausgewählt, in der Verwaltungskonsole ist die Option **Erweiterter KSN-Modus** ausgewählt), stimmen Sie durch das Akzeptieren der Bedingungen der Erklärung zu Kaspersky Security Network zu, Kaspersky zusätzlich zu den oben genannten Informationen automatisch die folgenden Informationen bereitzustellen.

Bereitstellung von Daten bei Verwendung des erweiterten KSN-Modus mit der Integration in Kaspersky Endpoint Detection and Response Expert (on-premises)

Wenn Sie Kaspersky Endpoint Security als Teil von Kaspersky Endpoint Detection and Response Expert (on-premises) verwenden und Kaspersky Security Network im erweiterten Modus nutzen, stimmen Sie durch das Akzeptieren der Bedingungen der Erklärung zu Kaspersky Security Network zu, Kaspersky zusätzlich zu den oben genannten Informationen automatisch die folgenden Informationen bereitzustellen.

Diese Daten werden bei Verwendung von Kaspersky Endpoint Security im Standard-Modus und im Modus „Endpoint Detection and Response Agent“ bereitgestellt

Wenn Sie Kaspersky Endpoint Security im Standard-Modus oder im Endpoint Detection and Response Agent-Modus sowie Kaspersky Security Network im erweiterten Modus verwenden, stimmen Sie durch das Akzeptieren der Bedingungen der Erklärung zu Kaspersky Security Network zu, Kaspersky zusätzlich zu den oben genannten Informationen automatisch die folgenden Informationen bereitzustellen:

Daten, die bei der Integration mit der Lösung "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:
  - Prozessname
  - Prozess-Argumente
  - Pfad zur ausführbaren Datei des Prozesses
  - Prozess-ID (PID)
  - ID des übergeordneten Prozesses (PPID)
  - Name des Benutzers, der den Prozess gestartet hat
  - Zeitpunkt (Datum und Uhrzeit), zu dem der Prozess gestartet wurde
- Informationen über Dienste:
  - Dienstname
  - Dienstbeschreibung
  - Pfad und Name der ausführbaren Dienstdatei
  - ID des Dienstes
  - Typ des Dienstes (Kernel-Treiber, Adapter usw.)
  - Dienststatus
  - Startmodus des Dienstes
  - Name des Benutzers, unter dem der Dienst gestartet wurde

- Informationen über das Dateisystem:
  - Volume-Name
  - Volume-Buchstabe
  - Volume-Typ
- 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:
  - Browsername
  - Browserversion
  - 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-Anforderung
  - Die eindeutige Kennung des Prozesses, der die HTTP-Anfrage gestellt hat.

Daten zum Erstellen einer Bedrohungsentwicklungskette

Daten zum Erstellen einer Bedrohungsentwicklungskette können die folgenden Informationen enthalten:

- Allgemeine Informationen zum dem Alarm:
  - Datum und Uhrzeit des Alarms
  - Name des Objekts
  - 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 (PPID)
  - 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
  - Dateiattribute eines 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, die die Datei heruntergeladen hat
- MD5- und SHA256-Hashsummen der Anwendung, von der die Datei heruntergeladen wurde
- Name der Anwendung, die die Datei zuletzt geändert hat
- 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
- Quelle der Links der verarbeiteten Webanfrage (HTTP-Referer)
- Benutzer-Agent der verarbeiteten Webanfrage
- Typ der verarbeiteten Webanfrage (GET oder POST)
- Lokaler IP-Port der verarbeiteten Webanfrage
- Remote-IP-Port der verarbeiteten Webanfrage
- Verbindungsrichtung (eingehend oder ausgehend) der verarbeiteten Webanfrage
- ID des Prozesses, in den der Schadcode eingeschleust wurde

Daten, die bei der Integration mit der Komponente "Kaspersky Endpoint Detection and Response (KATA)" bereitgestellt werden

Bei der Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response (KATA) als Teil der Lösung "Kaspersky Anti Targeted Attack Platform" speichert Kaspersky Endpoint Security die folgenden Informationen, welche möglicherweise personenbezogene und vertrauliche Daten enthalten:

- Adressen der Server mit Central Node-Komponente, welche die Interaktion mit Kaspersky Endpoint Detection and Response (KATA) (im Weiteren auch *KATA-Server*) gewährleisten.
- Öffentlicher Schlüssel des Serverzertifikats für die Integration mit Kaspersky Endpoint Detection and Response (KATA)
- Client-Zertifikat für die Integration mit Kaspersky Endpoint Detection and Response (KATA)
- Zugangsdaten für die Autorisierung auf dem Proxyserver.
- Parameter für die Häufigkeit der Synchronisation mit dem KATA-Server und Parameter für die Übertragung der Daten zum KATA-Server
- Verbindungsstatus mit dem KATA-Server und Informationen über Fehler in den Zertifikaten für Client und Server
- Parameter der von den KATA-Servern empfangenen Aufgaben:
  - Einstellungen des Zeitplans für den Aufgabenstart
  - Namen und Kennwörter der Benutzerkonten, unter denen die Aufgaben ausgeführt werden sollen
  - Versionen von Einstellungen
  - Start-Typ der Dienste
  - Namen der Dienste
  - Befehl (aus der Befehlszeile) zum Starten des Prozesses mit Argumenten
  - MD5- und SHA256-Hashes der verarbeiteten Objekte
  - Pfade zu Objekten
  - IOC-Dateien
- Einstellungen der Isolation, die verhindert, dass das Gerät nur mit den in den Ausnahmen angegeben Geräten kommunizieren kann.

Bei der Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response (KATA) werden von Kaspersky Endpoint Security die folgenden Informationen gespeichert und möglicherweise an den KATA-Server übertragen:

- Informationen aus den Synchronisationsanfragen an EDR Expert (on-premise):
  - Eindeutige ID
  - Basisteil der Server-Webadresse
  - Gerätename
  - IP-Adresse des Geräts
  - MAC-Adresse des Geräts
  - Lokale Uhrzeit des Geräts
  - Name und Version des auf dem Gerät installierten Betriebssystems
  - Version von Kaspersky Endpoint Security
  - Veröffentlichungsdatum der verwendeten Anwendungsdatenbanken
  - Status des Lizenzschlüssels.
- Informationen von Anfragen an EDR Expert (on-premise) in den Ergebnisberichten der Ausgabenausführung:
  - IP-Adresse des Geräts
  - Eindeutige ID
  - Basisteil der Server-Webadresse
  - MAC-Adresse des Geräts
  - Fehler bei der Aufgabenausführung und Rückgabecodes
  - Abschlussstatus der Aufgabe
  - Zeitpunkt, an dem die Aufgaben abgeschlossen wurden
  - Versionen der Parameter, mit denen Aufgaben ausgeführt wurden
  - Informationen über Prozesse, die auf Anfrage des Servers auf dem Gerät gestartet oder gestoppt wurden: PID und UniquePID, Fehlercode, MD5- und SHA256-Hash-Summen der Objekte
  - Vom Server angeforderte Dateien
  - Daten über Fehler beim Abrufen von Objektinformationen: vollständiger Name des Objekts, bei dessen Verarbeitung ein Fehler aufgetreten ist; Fehlercode
  - Aktivierungsstatus der Netzwerkisolation

- Für IOC-Indikatoren werden die Untersuchungsergebnisse zurückgegeben (wurde jeder Indikator ausgelöst oder nicht, gefundene Objekte und Informationen darüber, welcher Indikator-Branch ausgelöst wurde)
- Für Objekte, welche die IOC-Indikatoren auslösen, werden je nach Typ des Indikators unterschiedliche Werte zurückgegeben:
  - ArpEntry: IP-Adresse aus der ARP-Tabelle (einschließlich IPv6), physische Adresse aus der ARP-Tabelle
  - Datei: MD5-Hash der Datei, SHA256-Hash der Datei, vollständiger Dateiname (einschließlich Pfad), Dateigröße
  - Port: Remote-IP-Adresse und Port, mit dem während der Überprüfung eine Verbindung hergestellt wurde; IP-Adresse und Port des lokalen Adapters; Typ des Protokolls (TCP, UDP, IP, RAWIP)
  - Prozess: Name des Prozesses; Argumente des Prozesses; Pfad zur Prozessdatei; System-PID des Prozesses; System-PID des übergeordneten Prozesses; Name des Benutzers, unter dessen Namen der Prozess ausgeführt wird; Datum und Uhrzeit des Starts des Prozesses
  - SystemInfo: Name des Betriebssystems, Version des Betriebssystems, Netzwerkname des Geräts ohne Domäne, Domäne oder Arbeitsgruppe
  - Benutzer: Benutzername
- Für Objekte, die in die Quarantäne verschoben wurden:
  - Dateipfad
  - Dateigröße
  - Datei-ID, die dem Objekt beim Verschieben in die Quarantäne zugewiesen wurde
  - Flag-Indikator, dass die Originaldatei gelöscht wurde
- Für Dateien, die aus der Quarantäne abgerufen wurden:
  - Datei-ID, die dem Objekt beim Verschieben in die Quarantäne zugewiesen wurde
- Für verbotene Startvorgänge ausführbarer Dateien oder Skripte:
  - Prozess-ID
  - ID des übergeordneten Prozesses (PPID)
  - System-ID
  - ID der Anmeldesession am System
  - Status des Prozesses
  - Datum und Uhrzeit des unterbrochenen des Startvorgangs

- Für unterbundenes Öffnen von Dokumenten mittels Office-Anwendungen:
  - Prozess-ID
  - Datei-ID
  - Datum und Uhrzeit des unterbrochenen des Startvorgangs
- Informationen über Dateien:
  - Eindeutige Datei-ID
  - MD5-Hash des Objekts
  - Dateiinhalt
- Daten in Telemetriepaketen:
  - Informationen über Dateien:
    - Eindeutige Datei-ID
    - Dateipfad
    - Dateiname
    - Dateigröße
    - Datei-Attribute
    - Datum und Uhrzeit der Datei-Erstellung
    - Datum und Uhrzeit der letzten Datei-Änderung
    - MD5- und SHA256-Hashwerte des Objekts
    - Informationen über den Benutzer und die Gruppe, denen die Datei gehört (Name und ID)
  - Informationen zu laufenden Prozessen:
    - Datei-ID des Prozesses
    - Prozess-ID
    - Startparameter des Prozesses
    - Session-ID
    - Zeitpunkt (Datum und Uhrzeit), zu dem der Prozess gestartet wurde
    - Informationen über den Benutzer und die Gruppe, in deren Namen der Prozess ausgeführt wird (Name und ID)

- Informationen über den Prozess, der auf den Speicher eines anderen Prozesses zugreift:
  - Prozess-ID
  - Methode und Adresse der Implementierung (Injection)
  - Befehl (aus der Befehlszeile) zum Ändern des Prozesses mit Argumenten
  - Systemaufrufargumente des Prozesses
- Informationen zu erkannten und verarbeiteten Bedrohungen:
  - Der Name der erkannten Bedrohung und die Technologie, welche die Bedrohung erkannt hat, gemäß Kaspersky-Klassifizierung
  - Version der Anwendungsdatenbank
  - Webadresse, von der das infizierte Objekt heruntergeladen wurde
  - Status der Bedrohungsverarbeitung
  - Grund für das Scheitern einer Bedrohungsbeseitigung
  - Eindeutige ID der Dateibedrohung
- Daten über Dateiänderungen:
  - Eindeutige ID der geänderten Datei
  - Eindeutige ID des Prozesses, der die Änderungen vorgenommen hat
  - Informationen über die aufgetretene Änderung
- Informationen über Änderungen im System:
  - Eindeutige ID des Prozesses, der die Änderungen vorgenommen hat
  - Informationen über die aufgetretene Änderung
- Informationen über den am System angemeldeten Benutzer:
  - Session-ID
  - Informationen über den Benutzer (Name und ID)
  - IP-Adresse des Geräts, von welchem die Sitzung aufgebaut wurde
- Daten über beendende Prozesse: eindeutige Prozess-IDs
- Informationen zum Laden der Bibliothek in den Adressraum des Prozesses: ID der geladenen Bibliothek

- Informationen zu hergestellten Netzwerkverbindungen:
  - Lokale IP-Adresse
  - Remote-IP-Adresse
  - Richtung der Verbindung
  - Protokoll
- Informationen zu einem Prozess, der auf externe Netzwerkverbindungen an einem bestimmten Port "horcht":
  - Lokale Adresse (Port und IP-Adresse)
  - Protokoll
- Informationen über Zugriff auf den DNS-Server:
  - Domänenname der angeforderten Ressource
  - IP-Adresse der angeforderten Ressource
  - IP-Adresse des DNS-Servers
  - Anforderungstyp

Darüber hinaus können die angegebenen Informationen in den Protokoll- und Dump-Dateien gespeichert werden.

Daten, die bei der Integration mit der Komponente "Kaspersky Endpoint Detection and Response Expert (on-premise)" bereitgestellt werden

Bei Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Expert (on-premise) speichert Kaspersky Endpoint Security die folgenden Informationen, die persönliche und vertrauliche Daten enthalten können:

- Liste der Server für die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise).
- Öffentlicher Schlüssel des Zertifikats des Servers, der die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) bereitstellt.
- Client-Zertifikat für die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise).
- Zugangsdaten für die Autorisierung auf dem Proxyserver.
- Parameter für die Häufigkeit der Synchronisierung mit dem Server, der für die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) verantwortlich ist, sowie Parameter für die Datenübertragung an diesen Server.

- Status der Verbindung mit dem Server, der die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) verarbeitet, sowie Informationen über Fehler des Client- und Serverzertifikats.
- Parameter der Aufgaben, die von Servern für die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) eingehen:
  - Einstellungen des Zeitplans für den Aufgabenstart
  - Namen und Kennwörter der Benutzerkonten, unter denen die Aufgaben ausgeführt werden sollen
  - Versionen von Einstellungen
  - Start-Typ der Dienste
  - Namen der Dienste
  - Befehl (aus der Befehlszeile) zum Starten des Prozesses mit Argumenten
  - MD5- und SHA256-Hashes der verarbeiteten Objekte
  - Pfade zu Objekten
  - IOC-Dateien
- Einstellungen der Isolation, die verhindert, dass das Gerät nur mit den in den Ausnahmen angegeben Geräten kommunizieren kann.

Wenn die Anwendung Kaspersky Endpoint Security in Kaspersky Endpoint Detection and Response Expert (on-premise) integriert ist, speichert die Anwendung die folgenden Daten und kann sie an den Integrationsserver übertragen:

- Informationen aus Synchronisationsanfragen an die Komponente EDR Expert (on-premise):
  - Eindeutige ID
  - Basisteil der Server-Webadresse
  - Gerätename
  - IP-Adresse des Geräts
  - MAC-Adresse des Geräts
  - Lokale Uhrzeit des Geräts
  - Name und Version des auf dem Gerät installierten Betriebssystems
  - Version von Kaspersky Endpoint Security
  - Veröffentlichungsdatum der verwendeten Anwendungsdatenbanken
  - Status des Lizenzschlüssels.

- Informationen aus Anfragen an die Komponente EDR Expert (on-premise) in Berichten zur Aufgabenausführung:
  - IP-Adresse des Geräts
  - Eindeutige ID
  - Basisteil der Server-Webadresse
  - MAC-Adresse des Geräts
  - Fehler bei der Aufgabenausführung und Rückgabecodes
  - Abschlussstatus der Aufgabe
  - Zeitpunkt, an dem die Aufgaben abgeschlossen wurden
  - Versionen der Parameter, mit denen Aufgaben ausgeführt wurden
  - Informationen über Prozesse, die auf Anfrage des Servers auf dem Gerät gestartet oder gestoppt wurden: PID und UniquePID, Fehlercode, MD5- und SHA256-Hash-Summen der Objekte
  - Vom Server angeforderte Dateien
  - Daten über Fehler beim Abrufen von Objektinformationen: vollständiger Name des Objekts, bei dessen Verarbeitung ein Fehler aufgetreten ist; Fehlercode
  - Aktivierungsstatus der Netzwerkisolation
  - Für IOC-Indikatoren werden die Untersuchungsergebnisse zurückgegeben (wurde jeder Indikator ausgelöst oder nicht, gefundene Objekte und Informationen darüber, welcher Indikator-Branch ausgelöst wurde)
  - Für YARA-Regeln werden die Untersuchungsergebnisse zurückgegeben (ob die Regel ausgelöst wurde oder nicht, gefundene Objekte und Informationen darüber, welche Regel ausgelöst wurde)
  - Für Objekte, welche die IOC-Indikatoren auslösen, geben die YARA-Regeln je nach Typ unterschiedliche Werte zurück:
    - ArpEntry: IP-Adresse aus der ARP-Tabelle (einschließlich IPv6), physische Adresse aus der ARP-Tabelle
    - Datei: MD5-Hash der Datei, SHA256-Hash der Datei, vollständiger Dateiname (einschließlich Pfad), Dateigröße
    - Port: Remote-IP-Adresse und Port, mit dem während der Überprüfung eine Verbindung hergestellt wurde; IP-Adresse und Port des lokalen Adapters; Typ des Protokolls (TCP, UDP, IP, RAWIP)
    - Prozess: Name des Prozesses; Argumente des Prozesses; Pfad zur Prozessdatei; System-PID des Prozesses; System-PID des übergeordneten Prozesses; Name des Benutzers, unter dessen Namen der Prozess ausgeführt wird; Datum und Uhrzeit des Starts des Prozesses
    - SystemInfo: Name des Betriebssystems, Version des Betriebssystems, Netzwerkname des Geräts ohne Domäne, Domäne oder Arbeitsgruppe
    - Benutzer: Benutzername

- Für Objekte, die in die Quarantäne verschoben wurden:
  - Dateipfad
  - Dateigröße
  - Datei-IDs, die dem Objekt beim Verschieben in die Quarantäne zugewiesen wurde
  - Flag-Indikator, dass die Originaldatei gelöscht wurde
- Für Dateien, die aus der Quarantäne abgerufen, wiederhergestellt oder gelöscht wurden:
  - Datei-IDs, die dem Objekt beim Verschieben in die Quarantäne zugewiesen wurde
- Für verbotene Startvorgänge ausführbarer Dateien oder Skripte:
  - Prozess-ID
  - ID des übergeordneten Prozesses (PPID)
  - System-ID
  - ID der Anmeldesession am System
  - Status des Prozesses
  - Datum und Uhrzeit des unterbrochenen des Startvorgangs
- Für unterbundenes Öffnen von Dokumenten mittels Office-Anwendungen:
  - Prozess-ID
  - Datei-ID
  - Datum und Uhrzeit des unterbrochenen des Startvorgangs
- Liste der Dateien im angegebenen Verzeichnis:
  - Dateiname
  - Absoluter Pfad zur Datei
  - Dateigröße
  - Dateityp
  - Name und ID des Besitzers oder der Gruppe von Besitzern
  - Zugriffsrechte auf die Datei
  - Spezielle Dateisystem-Flags, die auf jede Datei angewendet werden
  - Metadaten zur Datei

    - Anzahl der Hardlinks zur Datei
    - Zeitpunkt der Erstellung, Änderung und des letzten Zugriffs auf die Datei
- Liste der gestarteten Prozesse auf dem Gerät:
    - Prozessname
    - Startzeitpunkt des Prozesses
    - Status des Prozesses
    - Prozess-ID (PID) und ID des übergeordneten Prozesses
    - Aktuelles Arbeitsverzeichnis des Prozesses
    - Startparameter des Prozesses
    - Umgebungsvariablen
    - Pfad zur ausführbaren Datei des Prozesses
    - Session-ID des Benutzers, der den Prozess gestartet hat
    - Benutzer-ID und Gruppen-ID, die den Prozess gestartet haben
    - Benutzer-ID und Gruppen-ID, mit deren Rechten der Prozess Zugriff auf Dateien und Ressourcen im System hat
- Liste der Autostart-Punkte:
    - Typ des Autostart-Punktes
    - Dateiname
    - Absoluter Pfad zur Datei
    - Zugriffsrechte auf die Datei
    - Spezielle Dateisystem-Flags, die auf jede Datei angewendet werden
    - Name und ID des Besitzers oder der Gruppe von Besitzern
    - Zeitpunkt der Erstellung, Änderung und des letzten Zugriffs auf die Datei
- Speicherabbild des Prozesses:
    - Prozessname
    - Vollständiger Pfad zur Datei des Prozesses
    - Dump-Datei des Prozesses
    - Größe der Dump-Datei des Prozesses

- Speicherabbild des Geräts: Dump-Datei des Arbeitsspeichers des Geräts
- Abbild der Festplatte des Geräts

- Informationen über Dateien:
  - Eindeutige Datei-ID
  - MD5-Hash des Objekts
  - Dateiinhalt

- Daten in Telemetriepaketen:
  - Informationen über Telemetrie-Ereignisse:
    - Ereignis-ID
    - Die laufende Nummer des Ereignisses in der Sequenz der gesendeten Telemetriepakete
    - Ereignistyp
    - Zeitpunkt des Auftretens des Ereignisses
  - Informationen über das geschützte Gerät
    - Name des geschützten Geräts
    - ID des geschützten Geräts in Kaspersky Security Center
    - ID des geschützten Geräts in Kaspersky Endpoint Detection and Response Expert (on-premise).
    - Name, Version und Familie des Betriebssystems auf dem geschützten Gerät
    - Zeitpunkt des Ein- und Ausschaltens des Betriebssystems auf dem geschützten Gerät
  - Informationen über Dateien:
    - Eindeutige Datei-ID
    - Dateipfad
    - Dateiname
    - Dateigröße
    - Datei-Attribute
    - Datum und Uhrzeit der Datei-Erstellung
    - Datum und Uhrzeit der letzten Datei-Änderung
    - MD5- und SHA256-Hashwerte des Objekts
    - Informationen über den Benutzer und die Gruppe, denen die Datei gehört (Name und ID)

- Informationen zu laufenden Prozessen:
  - Datei-ID des Prozesses
  - Prozess-ID
  - Startparameter des Prozesses
  - Session-ID
  - Zeitpunkt (Datum und Uhrzeit), zu dem der Prozess gestartet wurde
  - Informationen über den Benutzer und die Gruppe, in deren Namen der Prozess ausgeführt wird (Name und ID)
- Informationen über den Prozess, der auf den Speicher eines anderen Prozesses zugreift:
  - Prozess-ID
  - Methode und Adresse der Implementierung (Injection)
  - Befehl (aus der Befehlszeile) zum Ändern des Prozesses mit Argumenten
  - Systemaufrufargumente des Prozesses
- Informationen zu erkannten und verarbeiteten Bedrohungen:
  - Der Name der erkannten Bedrohung und die Technologie, welche die Bedrohung erkannt hat, gemäß Kaspersky-Klassifizierung
  - Veröffentlichungsdatum und Version der Anwendungsdatenbanken
  - Webadresse, von der das infizierte Objekt heruntergeladen wurde
  - Status der Bedrohungsverarbeitung
  - Grund für das Scheitern einer Bedrohungsbeseitigung
  - Eindeutige ID der Dateibedrohung
- Daten über Dateiänderungen:
  - Eindeutige ID der geänderten Datei
  - Eindeutige ID des Prozesses, der die Änderungen vorgenommen hat
  - Informationen über die aufgetretene Änderung
- Informationen über Änderungen im System:
  - Eindeutige ID des Prozesses, der die Änderungen vorgenommen hat
  - Informationen über die aufgetretene Änderung

- Informationen über den am System angemeldeten Benutzer:
  - Session-ID
  - Informationen über den Benutzer (Name und ID)
  - IP-Adresse des Geräts, von welchem die Sitzung aufgebaut wurde
- Daten über beendende Prozesse: eindeutige Prozess-IDs
- Informationen zum Laden der Bibliothek in den Adressraum des Prozesses: ID der geladenen Bibliothek
- Informationen zum Herstellen und Beenden einer Netzwerkverbindung:
  - Lokale IP-Adresse
  - Remote-IP-Adresse
  - Richtung der Verbindung
  - Protokoll
  - Zeitpunkt des Verbindungsaufbaus
  - Zeitpunkt der Verbindungsbeendigung
  - Verbindungsdauer
  - Während der Verbindung gesendete Bytes
  - Während der Verbindung empfangene Bytes
- Informationen zu einem Prozess, der auf externe Netzwerkverbindungen an einem bestimmten Port "horcht":
  - Lokale Adresse (Port und IP-Adresse)
  - Protokoll
- Informationen über Zugriff auf den DNS-Server:
  - Domänenname der angeforderten Ressource
  - IP-Adresse der angeforderten Ressource
  - IP-Adresse des DNS-Servers
  - Anforderungstyp
- Informationen über verbundene externe Geräte:
  - Typ des Vorgangs (Geräteverbindung)
  - Typ des Geräts
  - Eindeutige ID des Geräts

    - Gerätename
    - Pfad zum Gerät
- Informationen über die Anwendung und ihre Module:
    - Version der Anwendung
    - Zeitpunkte der Installation, des Starts, des Beendens und des Löschens der Anwendung
    - Initiator der Aktion für die Anwendung
    - Wenn Anwendung nicht ordnungsgemäß beendet: Ursache dafür
    - Wenn Anwendung nicht ordnungsgemäß beendet: Rückgabecodes
- Informationen zur Interaktion mit den Aufgabenplanern (Erstellen und Löschen von Aufgaben):
    - Aufgabenname
    - Pfad zum Befehl, der gemäß Zeitplan ausgeführt wird
    - Zeitplan für den Aufgabenstart
    - Name des Benutzerkontos, das die Aufgabe erstellt hat
    - Name des Kontos, unter dem die Aufgabe ausgeführt wird
    - Name des Benutzerkontos, das die Aufgabe gelöscht hat
- Informationen über das Erstellen, Löschen und Ändern von Diensten:
    - Name des Dienstes (einschließlich des vorherigen Namens, falls geändert)
    - Typ des Dienstes (einschließlich des vorherigen Typs, falls geändert)
    - Pfad zur ausführbaren Datei (einschließlich des vorherigen Pfads, falls geändert)
    - Abhängigkeiten des Dienstes (einschließlich vorheriger Abhängigkeiten, falls geändert)
    - Name des Benutzerkontos, unter dem der Dienst ausgeführt wird (einschließlich des vorherigen Namens, falls geändert)
    - Anzeigename des Dienstes (einschließlich des vorherigen Namens, falls geändert)
    - Name des Benutzerkontos, unter dem der Dienst erstellt, gelöscht oder geändert wurde
    - Kennzeichen für verzögertes Löschen
- Informationen über Eingaben in der Konsole:
    - ID und Typ des Prozesses, der die Konsoleneingabe initiiert hat
    - Inhalt der Eingabe in die Konsole

- Informationen über gemountete Gerät:
  - Systemname des Volumens
  - Mountpunkt
- Informationen über Änderungen im Prozessspeicher:
  - Systemaufrufargumente des Prozesses
  - Informationen über den Prozess, der den Code implementiert hat, und über seinen übergeordneten Prozess
    - ID und eindeutige ID des Prozesses und seines übergeordneten Prozesses
    - Befehlszeile, aus welcher der Prozess und sein übergeordneter Prozess gestartet wurden
    - Umgebungsvariablen des Prozesses
    - Art des Benutzerkontos, unter dessen Namen der Prozess und der übergeordnete Prozess gestartet wurden
    - Systemaufruf, mit dem der Prozess erstellt wurde
    - Benutzer-ID und Gruppen-ID, die den Prozess gestartet haben
    - Name und vollständiger Name des Prozesses und des übergeordneten Prozesses
    - Vollständiger Pfad zum Prozess und zum übergeordneten Prozess
    - MD5- und SHA256-Hashes des Prozesses und des übergeordneten Prozesses
    - Session-ID
    - Name, Domänenname und Benutzer-ID, die den Prozess und den übergeordneten Prozess gestartet haben
  - Informationen über den Prozess, durch den der Prozess geladen wurde, der den Code implementiert hat
    - Eindeutige Prozess-ID, durch die der Prozess geladen wurde
    - Name und vollständiger Name der Datei, durch die der Prozess geladen wurde
    - Vollständiger Pfad zum Prozess, durch den der Prozess geladen wurde
    - MD5-Hash des Prozesses, durch den der Prozess geladen wurde
  - Informationen über den Prozess, der den Prozess initiiert hat
    - ID und eindeutige ID des Prozesses, der den Prozess initiiert hat
    - Befehlszeile des Prozesses, der den Prozess initiiert hat
    - Name und Domänenname des Benutzers, der den Prozess gestartet hat, der den Prozess initiiert hat

- Name und vollständiger Name des Prozesses, der den Prozess initiiert hat
- Vollständiger Pfad zum Prozess, der den Prozess initiiert hat
- MD5- und SHA256-Hashes des Prozesses, der den Prozess initiiert hat

Darüber hinaus können die angegebenen Informationen in den Protokoll- und Dump-Dateien gespeichert werden.

Daten, die bei der Integration mit der Komponente Kaspersky Endpoint Detection and Response Expert (cloud) bereitgestellt werden

Bei der Integration von Kaspersky Endpoint Security in Kaspersky Endpoint Detection and Response Expert (cloud) speichert Kaspersky Endpoint Security die folgenden Informationen, die personenbezogene und vertrauliche Daten enthalten können:

- Liste der Server für die Integration in Kaspersky Endpoint Detection and Response Expert (cloud).
- Adressen der Tunnel der Telemetrie- und Response-Server für Kaspersky Endpoint Detection and Response Expert (cloud).
- Serverzertifikat für die Integration in Kaspersky Endpoint Detection and Response Expert (cloud).
- Client-Zertifikat für die Integration in Kaspersky Endpoint Detection and Response Expert (cloud).
- Einstellungen für die Häufigkeit der Synchronisierung mit dem Server, der für die Integration in Kaspersky Endpoint Detection and Response Expert (cloud) verantwortlich ist, sowie Einstellungen für die Datenübertragung für diesen Server.
- Status der Verbindung zum Server, der die Integration in Kaspersky Endpoint Detection and Response Expert (cloud) verarbeitet, sowie Informationen über Fehler bei Client- und Serverzertifikaten.
- Parameter der Aufgaben, die von Servern für die Integration in Kaspersky Endpoint Detection and Response Expert (cloud) stammen:
  - Einstellungen des Zeitplans für den Aufgabenstart
  - Namen und Kennwörter der Benutzerkonten, unter denen die Aufgaben ausgeführt werden sollen
  - Versionen von Einstellungen
  - Start-Typ der Dienste
  - Namen der Dienste
  - Befehl (aus der Befehlszeile) zum Starten des Prozesses mit Argumenten
  - MD5- und SHA256-Hashes der verarbeiteten Objekte

- Pfade zu Objekten
- IOC-Dateien

- Einstellungen der Isolation, die verhindert, dass das Gerät nur mit den in den Ausnahmen angegeben Geräten kommunizieren kann.

Wenn die Anwendung Kaspersky Endpoint Security in Kaspersky Endpoint Detection and Response Expert (cloud) integriert ist, speichert die Anwendung die folgenden Daten und kann sie an den Integrationsserver übertragen:

- Informationen für Synchronisierungsanfragen an die Komponente EDR Expert (cloud):
  - Eindeutige ID
  - Basisteil der Server-Webadresse
  - Gerätename
  - IP-Adresse des Geräts
  - MAC-Adresse des Geräts
  - Lokale Uhrzeit des Geräts
  - Name und Version des auf dem Gerät installierten Betriebssystems
  - Version von Kaspersky Endpoint Security
  - Veröffentlichungsdatum der verwendeten Anwendungsdatenbanken
  - Status des Lizenzschlüssels.
- Informationen aus Anfragen an die Komponente EDR Expert (cloud) in Berichten zur Aufgabenausführung:
  - IP-Adresse des Geräts
  - Eindeutige ID
  - Basisteil der Server-Webadresse
  - MAC-Adresse des Geräts
  - Fehler bei der Aufgabenausführung und Rückgabecodes
  - Abschlussstatus der Aufgabe
  - Zeitpunkt, an dem die Aufgaben abgeschlossen wurden
  - Versionen der Parameter, mit denen Aufgaben ausgeführt wurden

- Informationen über Prozesse, die auf Anforderung des Servers auf dem Gerät gestartet wurden:
  - Prozessbeendigungscode
  - Eindeutige ID der Standardausgabedatei des Prozesses.
  - Eindeutige ID der Standardfehlerdatei des Prozesses.
- Informationen über Prozesse, die auf Anforderung des Servers auf dem Gerät gestartet oder beendet wurden:
  - PID (Systemprozess-ID).
  - UniquePID (eindeutige Kennung des Prozesses)
  - Fehlercode
- Kopie der vom Server angeforderten Datei sowie der Pfad zur Datei und ihre ID.
- Flag zum Löschen der Datei nach dem Neustart des Betriebssystems.
- Daten über Fehler beim Abrufen von Objektinformationen: vollständiger Name des Objekts, bei dessen Verarbeitung ein Fehler aufgetreten ist; Fehlercode
- Aktivierungsstatus der Netzwerkisolation
- Für IOC-Indikatoren werden die Untersuchungsergebnisse zurückgegeben (wurde jeder Indikator ausgelöst oder nicht, gefundene Objekte und Informationen darüber, welcher Indikator-Branch ausgelöst wurde)
- Für Objekte, in denen IoCs erkannt wurden, werden je nach Indikatortyp unterschiedliche Werte zurückgegeben:
  - ArpEntry: IP-Adresse aus der ARP-Tabelle (einschließlich IPv6), physische Adresse aus der ARP-Tabelle
  - Datei: MD5-Hash der Datei, SHA256-Hash der Datei, vollständiger Dateiname (einschließlich Pfad), Dateigröße
  - Port: Remote-IP-Adresse und Port, mit dem während der Überprüfung eine Verbindung hergestellt wurde; IP-Adresse und Port des lokalen Adapters; Typ des Protokolls (TCP, UDP, IP, RAWIP)
  - Prozess: Name des Prozesses; Argumente des Prozesses; Pfad zur Prozessdatei; System-PID des Prozesses; System-PID des übergeordneten Prozesses; Name des Benutzers, unter dessen Namen der Prozess ausgeführt wird; Datum und Uhrzeit des Starts des Prozesses
  - SystemInfo: Name des Betriebssystems, Version des Betriebssystems, Netzwerkname des Geräts ohne Domäne, Domäne oder Arbeitsgruppe
  - Benutzer: Benutzername
- Für Objekte, die in die Quarantäne verschoben wurden:
  - Dateipfad
  - Dateigröße

    - Datei-IDs, die dem Objekt beim Verschieben in die Quarantäne zugewiesen wurde
    - Flag-Indikator, dass die Originaldatei gelöscht wurde
- Für Dateien, die aus der Quarantäne abgerufen, wiederhergestellt oder gelöscht wurden:
    - Datei-IDs, die dem Objekt beim Verschieben in die Quarantäne zugewiesen wurde
- Für verbotene Startvorgänge ausführbarer Dateien oder Skripte:
    - Prozess-ID
    - ID des übergeordneten Prozesses (PPID)
    - System-ID
    - ID der Anmeldesession am System
    - Status des Prozesses
    - Datum und Uhrzeit des unterbrochenen des Startvorgangs
- Für unterbundenes Öffnen von Dokumenten mittels Office-Anwendungen:
    - Prozess-ID
    - Datei-ID
    - Datum und Uhrzeit des unterbrochenen des Startvorgangs
- Liste der Dateien im angegebenen Verzeichnis:
    - Dateiname
    - Absoluter Pfad zur Datei
    - Dateigröße
    - Dateityp
    - Name und ID des Besitzers oder der Gruppe von Besitzern
    - Zugriffsrechte auf die Datei
    - Spezielle Dateisystem-Flags, die auf jede Datei angewendet werden
    - Metadaten zur Datei
    - Anzahl der Hardlinks zur Datei
    - Zeitpunkt der Erstellung, Änderung und des letzten Zugriffs auf die Datei

- Liste der gestarteten Prozesse auf dem Gerät:
  - Prozessname
  - Startzeitpunkt des Prozesses
  - Status des Prozesses
  - Prozess-ID (PID) und ID des übergeordneten Prozesses
  - Aktuelles Arbeitsverzeichnis des Prozesses
  - Startparameter des Prozesses
  - Umgebungsvariablen
  - Pfad zur ausführbaren Datei des Prozesses
  - Session-ID des Benutzers, der den Prozess gestartet hat
  - Benutzer-ID und Gruppen-ID, die den Prozess gestartet haben
  - Benutzer-ID und Gruppen-ID, mit deren Rechten der Prozess Zugriff auf Dateien und Ressourcen im System hat
- Liste der Autostart-Punkte:
  - Typ des Autostart-Punktes
  - Dateiname
  - Absoluter Pfad zur Datei
  - Zugriffsrechte auf die Datei
  - Spezielle Dateisystem-Flags, die auf jede Datei angewendet werden
  - Name und ID des Besitzers oder der Gruppe von Besitzern
  - Zeitpunkt der Erstellung, Änderung und des letzten Zugriffs auf die Datei
  - MD5-Hash und SHA-256-Hash der ausführbaren Datei oder des ladbaren Moduls.
- Speicherabbild des Prozesses:
  - Name der Speicherabbilddatei des Prozesses.
  - Vollständiger Pfad zur Datei des Prozesses
  - Eindeutige ID der Speicherabbilddatei des Prozesses.
  - Größe der Speicherabbilddatei des Prozesses.

- Speicherabbild des Geräts:
  - Datum und Uhrzeit des Beginns der Dump-Erstellung.
  - Vollständiger Pfad zur Dump-Datei
  - Größe der Speicherabbilddatei des Geräts.
- Datenträgerabbild des Geräts:
  - Datum und Uhrzeit des Beginns der Dump-Erstellung.
  - Array mit vollständigen Pfaden zu den Dump-Dateien
  - Größe der Datenträgerabbilddatei des Geräts.
  - Logischer Datenträger.
  - Physischer Datenträger.
- Daten in Telemetriepaketen:
  - Informationen über Telemetrie-Ereignisse:
    - Ereignis-ID
    - Die laufende Nummer des Ereignisses in der Sequenz der gesendeten Telemetriepakete
    - Ereignistyp
    - Zeitpunkt des Auftretens des Ereignisses
  - Informationen über das geschützte Gerät
    - Name des geschützten Geräts
    - ID des geschützten Geräts in Kaspersky Security Center
    - ID des geschützten Geräts in Kaspersky Endpoint Detection and Response Expert (on-premise).
    - Name, Version und Familie des Betriebssystems auf dem geschützten Gerät
    - Zeitpunkt des Ein- und Ausschaltens des Betriebssystems auf dem geschützten Gerät
  - Informationen über Dateien:
    - Eindeutige Datei-ID
    - Dateipfad
    - Dateiname
    - Dateigröße
    - Datei-Attribute

    - Datum und Uhrzeit der Datei-Erstellung
    - Datum und Uhrzeit der letzten Datei-Änderung
    - MD5- und SHA256-Hashwerte des Objekts
    - Informationen über den Benutzer und die Gruppe, denen die Datei gehört (Name und ID)
- Informationen zu laufenden Prozessen:
    - Datei-ID des Prozesses
    - Prozess-ID
    - Startparameter des Prozesses
    - Session-ID
    - Zeitpunkt (Datum und Uhrzeit), zu dem der Prozess gestartet wurde
    - Informationen über den Benutzer und die Gruppe, in deren Namen der Prozess ausgeführt wird (Name und ID)
- Informationen über den Prozess, der auf den Speicher eines anderen Prozesses zugreift:
    - Prozess-ID
    - Methode und Adresse der Implementierung (Injection)
    - Befehl (aus der Befehlszeile) zum Ändern des Prozesses mit Argumenten
    - Systemaufrufargumente des Prozesses
- Informationen zu erkannten und verarbeiteten Bedrohungen:
    - Der Name der erkannten Bedrohung und die Technologie, welche die Bedrohung erkannt hat, gemäß Kaspersky-Klassifizierung
    - Veröffentlichungsdatum und Version der Anwendungsdatenbanken
    - Webadresse, von der das infizierte Objekt heruntergeladen wurde
    - Status der Bedrohungsverarbeitung
    - Grund für das Scheitern einer Bedrohungsbeseitigung
    - Eindeutige ID der Dateibedrohung
- Daten über Dateiänderungen:
    - Eindeutige ID der geänderten Datei
    - Eindeutige ID des Prozesses, der die Änderungen vorgenommen hat
    - Informationen über die aufgetretene Änderung

- Informationen über Änderungen im System:
  - Eindeutige ID des Prozesses, der die Änderungen vorgenommen hat
  - Informationen über die aufgetretene Änderung
- Informationen über den am System angemeldeten Benutzer:
  - Session-ID
  - Informationen über den Benutzer (Name und ID)
  - IP-Adresse des Geräts, von welchem die Sitzung aufgebaut wurde
- Daten über beendende Prozesse: eindeutige Prozess-IDs
- Informationen zum Laden der Bibliothek in den Adressraum des Prozesses: ID der geladenen Bibliothek
- Informationen zum Herstellen und Beenden einer Netzwerkverbindung:
  - Lokale IP-Adresse
  - Remote-IP-Adresse
  - Richtung der Verbindung
  - Protokoll
  - Zeitpunkt des Verbindungsaufbaus
  - Zeitpunkt der Verbindungsbeendigung
  - Verbindungsdauer
  - Während der Verbindung gesendete Bytes
  - Während der Verbindung empfangene Bytes
- Informationen zu einem Prozess, der auf externe Netzwerkverbindungen an einem bestimmten Port "horcht":
  - Lokale Adresse (Port und IP-Adresse)
  - Protokoll
- Informationen über Zugriff auf den DNS-Server:
  - Domänenname der angeforderten Ressource
  - IP-Adresse der angeforderten Ressource
  - IP-Adresse des DNS-Servers
  - Anforderungstyp

- Informationen über verbundene externe Geräte:
  - Typ des Vorgangs (Geräteverbindung)
  - Typ des Geräts
  - Eindeutige ID des Geräts
  - Gerätename
  - Pfad zum Gerät
- Informationen über die Anwendung und ihre Module:
  - Version der Anwendung
  - Zeitpunkte der Installation, des Starts, des Beendens und des Löschens der Anwendung
  - Initiator der Aktion für die Anwendung
  - Wenn Anwendung nicht ordnungsgemäß beendet: Ursache dafür
  - Wenn Anwendung nicht ordnungsgemäß beendet: Rückgabecodes
- Informationen zur Interaktion mit den Aufgabenplanern (Erstellen und Löschen von Aufgaben):
  - Aufgabenname
  - Pfad zum Befehl, der gemäß Zeitplan ausgeführt wird
  - Zeitplan für den Aufgabenstart
  - Name des Benutzerkontos, das die Aufgabe erstellt hat
  - Name des Kontos, unter dem die Aufgabe ausgeführt wird
  - Name des Benutzerkontos, das die Aufgabe gelöscht hat
- Informationen über das Erstellen, Löschen und Ändern von Diensten:
  - Name des Dienstes (einschließlich des vorherigen Namens, falls geändert)
  - Typ des Dienstes (einschließlich des vorherigen Typs, falls geändert)
  - Pfad zur ausführbaren Datei (einschließlich des vorherigen Pfads, falls geändert)
  - Abhängigkeiten des Dienstes (einschließlich vorheriger Abhängigkeiten, falls geändert)
  - Name des Benutzerkontos, unter dem der Dienst ausgeführt wird (einschließlich des vorherigen Namens, falls geändert)
  - Anzeigename des Dienstes (einschließlich des vorherigen Namens, falls geändert)

- Name des Benutzerkontos, unter dem der Dienst erstellt, gelöscht oder geändert wurde
- Kennzeichen für verzögertes Löschen

- Informationen über Eingaben in der Konsole:
  - ID und Typ des Prozesses, der die Konsoleneingabe initiiert hat
  - Inhalt der Eingabe in die Konsole
- Informationen über gemountete Gerät:
  - Systemname des Volumens
  - Mountpunkt
- Informationen über Änderungen im Prozessspeicher:
  - Systemaufrufargumente des Prozesses
  - Informationen über den Prozess, der den Code implementiert hat, und über seinen übergeordneten Prozess
    - ID und eindeutige ID des Prozesses und seines übergeordneten Prozesses
    - Befehlszeile, aus welcher der Prozess und sein übergeordneter Prozess gestartet wurden
    - Umgebungsvariablen des Prozesses
    - Art des Benutzerkontos, unter dessen Namen der Prozess und der übergeordnete Prozess gestartet wurden
    - Systemaufruf, mit dem der Prozess erstellt wurde
    - Benutzer-ID und Gruppen-ID, die den Prozess gestartet haben
    - Name und vollständiger Name des Prozesses und des übergeordneten Prozesses
    - Vollständiger Pfad zum Prozess und zum übergeordneten Prozess
    - MD5- und SHA256-Hashes des Prozesses und des übergeordneten Prozesses
    - Session-ID
    - Name, Domänenname und Benutzer-ID, die den Prozess und den übergeordneten Prozess gestartet haben
  - Informationen über den Prozess, durch den der Prozess geladen wurde, der den Code implementiert hat
    - Eindeutige Prozess-ID, durch die der Prozess geladen wurde
    - Name und vollständiger Name der Datei, durch die der Prozess geladen wurde

- Vollständiger Pfad zum Prozess, durch den der Prozess geladen wurde
- MD5-Hash des Prozesses, durch den der Prozess geladen wurde

- Informationen über den Prozess, der den Prozess initiiert hat
  - ID und eindeutige ID des Prozesses, der den Prozess initiiert hat
  - Befehlszeile des Prozesses, der den Prozess initiiert hat
  - Name und Domänenname des Benutzers, der den Prozess gestartet hat, der den Prozess initiiert hat
  - Name und vollständiger Name des Prozesses, der den Prozess initiiert hat
  - Vollständiger Pfad zum Prozess, der den Prozess initiiert hat
  - MD5- und SHA256-Hashes des Prozesses, der den Prozess initiiert hat

Darüber hinaus können die angegebenen Informationen in den Protokoll- und Dump-Dateien gespeichert werden.

Daten, die bei der Integration mit der Komponente "Kaspersky Network Detection and Response (KATA)" bereitgestellt werden

Bei der Integration von Kaspersky Endpoint Security mit der Komponente "Kaspersky Network Detection and Response" (KATA) als Teil der Lösung "Kaspersky Anti Targeted Attack Platform" speichert Kaspersky Endpoint Security die folgenden Informationen, welche möglicherweise personenbezogene und vertrauliche Daten enthalten:

- Adressen der NDR-Server.
- Öffentlicher Schlüssel des Serverzertifikats für die Integration mit Kaspersky Network Detection and Response (KATA).
- Client-Zertifikat für die Integration mit Kaspersky Network Detection and Response (KATA).
- Zugangsdaten für die Autorisierung auf dem Proxyserver.
- Parameter für die Häufigkeit der Synchronisation mit dem NDR-Server und Parameter für die Übertragung der Daten zum NDR-Server
- Verbindungsstatus mit dem NDR-Server und Informationen über Fehler in den Zertifikaten für Client und Server.

Bei der Integration von Kaspersky Endpoint Security mit der Komponente "Kaspersky Network Detection and Response" (KATA) werden von Kaspersky Endpoint Security die folgenden Informationen gespeichert und an den NDR-Server übertragen:

- Daten aus Synchronisationsanfragen an den NDR-Server:
  - Eindeutige ID
  - Basisteil der Server-Webadresse

- Gerätename
- IP-Adresse des Geräts
- MAC-Adresse des Geräts
- Lokale Uhrzeit des Geräts
- Name, Familie und Version des auf dem Gerät installierten Betriebssystems
- Version von Kaspersky Endpoint Security
- Veröffentlichungsdatum der verwendeten Anwendungsdatenbanken
- Status des Lizenzschlüssels.
- Modell und Hersteller des Geräts des Benutzers.

- Daten in Telemetriepaketen:
  - Informationen über Gerät und Benutzer:
    - Name des Geräts und Uhrzeit auf dem Gerät
    - Name, Familie und Version des Betriebssystems
    - Informationen zu den Netzwerkschnittstellen (Beschreibung, Liste der IP-Adressen mit Subnetzmaske, MAC-Adresse, metrische Nummer, DNS-Domänenname, Routing-Informationen, Nummern abgehorchter Ports)
    - Interne eindeutige Geräte-ID
    - Namen und IDs der Benutzer
    - Namen und IDs der Benutzergruppen
  - Informationen über die Anwendung Kaspersky Endpoint Security:
    - Name und Version der Anwendung
    - Datum der letzten Aktualisierung der Anwendung
    - Informationen über Lizenzschlüssel (Seriennummer, Typ, Gültigkeitsdauer der Lizenz, Status des Schlüssels)
    - Version der Anwendungsdatenbank
    - Liste der unterstützten API-Versionen
  - Informationen über bestehende Verbindungen:
    - Lokale IP-Adresse, Port und MAC-Adresse
    - Remote-IP-Adresse, Port und MAC-Adresse

    - IP-Adresse des Gateways
    - Typ des Protokolls (IANA), Nummer des Protokolls und EtherType
    - Anzahl der empfangenen und gesendeten Pakete
- Informationen über verarbeitete Dateien:
    - Name und eindeutige ID einer Datei
    - Typ und Größe der Datei
    - Vollständiger Pfad zum Image der Datei
    - Attributmaske des Dateisystems
    - Zeitpunkte der Erstellung und Änderung der Datei
    - Prüfsummen (MD5 und SHA256)
    - Berechtigungen der Dateiberechtigungen, einschließlich geerbter und wirksamer Berechtigungen.
- Informationen über gestartete und beendete Prozesse:
    - UID und PID eines Prozesses
    - Prozesstyp.
    - Session-ID
    - Auszuführender Befehl
    - Umgebungsvariablen
- Informationen zu erkannten und verarbeiteten Bedrohungen:
    - Der Name der erkannten Bedrohung und die Technologie, welche die Bedrohung erkannt hat, gemäß Kaspersky-Klassifizierung
    - Version der Anwendungsdatenbank
    - Webadresse, von der das infizierte Objekt heruntergeladen wurde
    - Status der Bedrohungsverarbeitung
    - Grund für das Scheitern einer Bedrohungsbeseitigung

Darüber hinaus können die angegebenen Informationen in den Protokoll- und Dump-Dateien gespeichert werden.

Daten, die bei der Integration mit der Lösung "Kaspersky Unified Monitoring and Analysis Platform" bereitgestellt werden

Bei Integration der Anwendung "Kaspersky Endpoint Security" mit der Lösung "Kaspersky Unified Monitoring and Analysis Platform" speichert Kaspersky Endpoint Security die folgenden Informationen, die persönliche und vertrauliche Daten enthalten können:

- Adressen der KUMA-Server.
- Öffentlicher Schlüssel des Serverzertifikats für die Integration mit der Kaspersky Unified Monitoring and Analysis Platform (außer, wenn für die Verbindung mit dem KUMA-Server das UDP-Protokoll verwendet wird).
- Client-Zertifikat für die Integration mit der Kaspersky Unified Monitoring and Analysis Platform.
- Zugangsdaten für die Autorisierung auf dem Proxyserver.
- Parameter für die Häufigkeit der Synchronisation mit dem KUMA-Server und Parameter für die Übertragung der Daten zum KUMA-Server
- Verbindungsstatus mit dem KUMA-Server und Informationen über Fehler in den Zertifikaten für Client und Server.

Bei Integration der Anwendung "Kaspersky Endpoint Security" mit der Lösung "Kaspersky Unified Monitoring and Analysis Platform" werden von Kaspersky Endpoint Security die folgenden Daten gespeichert und in Form von Telemetriedaten-Paketen an den KUMA-Server übertragen:

- Informationen über Veränderungen an Dateien:
  - Eindeutige ID der Datei vor der Änderung
  - Eindeutige ID der geänderten Datei
  - Eindeutige ID des Prozesses, der die Änderungen vorgenommen hat
  - Typ und Flag-Indikator des Vorgangs mit der Datei
  - Datum und Uhrzeit der Datei-Änderung
- Informationen über gestartete und beendete Prozesse:
  - Datei-ID des Prozesses
  - UID und PID eines Prozesses
  - Startparameter des Prozesses
  - Session-ID
  - Zeitpunkt (Datum und Uhrzeit), zu dem der Prozess gestartet wurde
  - Informationen über den Benutzer und die Gruppe, in deren Namen der Prozess ausgeführt wird (Name und ID)

- Informationen zu Ereignissen im Ereignisprotokoll:
  - Datum und Uhrzeit, an dem Ereignis aufgetreten ist
  - UID des Prozesses, der dem Ereignis zugeordnet ist
  - Typ und Beschreibung des Ereignisses
  - Ergebnis des ausgeführten Vorgangs

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.

Markenrechtliche Hinweise

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

Adobe, Acrobat, Flash und Shockwave sind entweder eingetragene Markenzeichen oder Markenzeichen von Adobe in den USA und/oder anderen Ländern.

AMD64 ist ein Markenzeichen oder eingetragenes Markenzeichen von Advanced Micro Devices, Inc.

Amazon ist ein Markenzeichen von Amazon.com, Inc. oder seinen verbundenen Unternehmen.

Arm ist ein eingetragenes Markenzeichen von Arm Limited (oder seinen Tochtergesellschaften) in den Vereinigten Staaten und/oder anderen Ländern.

AutoCAD ist ein Markenzeichen oder eingetragenes Markenzeichen von Autodesk, Inc. und/oder deren Tochterunternehmen und/oder verbundenen Unternehmen in den USA und/oder anderen Ländern.

Borland ist ein Markenzeichen oder ein eingetragenes Markenzeichen der Borland Software Corporation.

dBase ist eine Marke der dataBased Intelligence, Inc.

FireWire ist eine Markenzeichen von Apple Inc.

Die Bluetooth-Wortmarke, das Markenzeichen und die Bluetooth-Logos sind Eigentum von Bluetooth SIG, Inc.

Ubuntu und LTS sind eingetragene Markenzeichen von Canonical Ltd.

XenServer ist eine eingetragenes Markenzeichen oder ein Markenzeichen der Cloud Software Group, Inc. und/oder ihren Tochtergesellschaften in den Vereinigten Staaten und/oder anderen Ländern.

Cloudflare, das Cloudflare-Logo und Cloudflare Workers sind Markenzeichen und/oder eingetragene Markenzeichen von Cloudflare, Inc. in den USA und anderen Jurisdiktionen.

Die Wortmarke Grafana und das Grafana-Logo sind registrierte Markenzeichen/Dienstleistungsmarkenzeichen oder Markenzeichen/Dienstleistungsmarkenzeichen von Coding Instinct AB in den USA und anderen Ländern und werden mit Erlaubnis von Coding Instinct verwendet. Wir sind weder eine verbundene, unterstützte noch gesponserte Firma von Coding Instinct oder der Grafana-Gesellschaft.

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 besitzen möglicherweise auch Rechte an Markenzeichen, die durch andere, in diesem Dokument verwendete Begriffe, beschrieben werden.

Chrome, Chromium, Google Chrome und Google Public DNS sind Markenzeichen von Google LLC.

HUAWEI, EulerOS und FusionSphere sind Markenzeichen der Huawei Technologies Co., Ltd.

Linux ist ein in den USA und/oder in anderen Ländern eingetragenes Markenzeichen von Linus Torvalds.

Microsoft, Microsoft Edge, Active Directory, Hyper-V, Outlook, Visual Basic, Visual FoxPro, Visual C++, PowerPoint, Excel, Internet Explorer, Windows und Windows Server sind Markenzeichen der Microsoft-Unternehmensgruppe.

OpenStack ist ein eingetragenes Markenzeichen der OpenStack Foundation in den USA und anderen Ländern.

Oracle, Java und JavaScript sind eingetragene Markenzeichen von Oracle und/oder seinen verbundenen Unternehmen.

Python ist ein Markenzeichen oder eingetragenes Markenzeichen der Python Software Foundation.

Red Hat Enterprise Linux, CentOS und Fedora sind Markenzeichen oder eingetragene Markenzeichen von Red Hat, Inc. oder deren Tochterunternehmen in den USA und anderen Ländern.

Debian ist ein eingetragenes Markenzeichen von Software in the Public Interest, Inc.

Kubernetes ist ein eingetragenes Markenzeichen der The Linux Foundation in den Vereinigten Staaten und anderen Ländern.

Rocky Linux ist ein Markenzeichen der The Rocky Enterprise Software Foundation.

UNIX ist ein in den USA und in anderen Ländern eingetragenes Markenzeichen, dessen Nutzung von X/Open Company Limited lizenziert wird.

Zabbix ist eine eingetragenes Markezeichen von Zabbix SIA.