kaspersky

Kaspersky Endpoint Security für Linux

© 2026 AO Kaspersky Lab

Inhalt

Hilfe von Kaspersky Endpoint Security 12.4 für Linux

Über Kaspersky Endpoint Security 12.4 für Linux

- Über die Nutzungsmodi von Kaspersky Endpoint Security
  - Anwendung im Light Agent-Modus verwenden
  - Anwendung im Modus als Endpoint Detection and Response Agent verwenden
- Lieferumfang
- Hard- und Softwarevoraussetzungen
  - Hardwarevoraussetzungen
  - Softwarevoraussetzungen
  - Zusätzliche Software-Anforderungen für den Light Agent-Modus
  - Unterstützte Versionen von Kaspersky Security Center
  - Unterstützte Versionen der Lösung auf den KATA- und OSMP-Plattformen

Neuerungen

Behobene Probleme

Vorbereitung der Installation von Kaspersky Endpoint Security

Installation und Erstkonfiguration von Kaspersky Endpoint Security

- Installation und Erstkonfiguration des Administrationsagenten von Kaspersky Security Center
- Verwaltungs-Plug-ins für Kaspersky Endpoint Security installieren
  - Web-Plug-in für Kaspersky Endpoint Security installieren
  - MMC-Plug-in für Kaspersky Endpoint Security installieren
- Installation und Erstkonfiguration der Anwendung mithilfe von Kaspersky Security Center
  - Ein Installationspaket in der Web Console erstellen
  - Parameter für die Erstkonfiguration in der Web Console
  - Ein Installationspaket in der Administrationskonsole erstellen
  - Parameter für die Erstkonfiguration in der Verwaltungskonsole
  - Vorbereitung eines Archivs mit Anwendungsdatenbanken zur Erstellung eines Installationspakets mit integrierten Datenbanken
  - Parameter der Konfigurationsdatei "autoinstall.ini"
  - Anwendung für die gemeinsame Ausführung mit Kaspersky Security Center vorbereiten
- Installation und Erstkonfiguration der Anwendung über die Befehlszeile
  - Anwendung über die Befehlszeile installieren
  - Erstkonfiguration der Anwendung im interaktiven Modus
    - Anwendungsmodus auswählen: Standard oder Light Agent
    - Rolle der virtuellen Maschine festlegen
    - Modus zum Schutz der VDI-Infrastruktur aktivieren
    - Verwendungsmodus auswählen: Standard oder Endpoint Detection and Response Agent
    - Sprachstandard auswählen
    - Endbenutzer-Lizenzvertrag und Datenschutzrichtlinie lesen
    - Endbenutzer-Lizenzvertrag annehmen
    - Akzeptieren der Datenschutzrichtlinie
    - Verwendung von Kaspersky Security Network
    - Benutzer aus privilegierten Gruppen entfernen
    - Einem Benutzer die Administratorrolle zuweisen

Mechanismus zum Abfangen von Systemereignissen konfigurieren
Automatische SELinux-Konfiguration aktivieren
Update-Quelle konfigurieren
Allgemeine Proxy-Server-Einstellungen anpassen
Update der Anwendungsdatenbanken starten
Automatische Updates für die Anwendungsdatenbanken aktivieren
Programm aktivieren
Erstkonfiguration der Anwendung im automatischen Modus
Einstellungen der Konfigurationsdatei für die Erstkonfiguration des Programms
Zulassungsregeln im SELinux-System konfigurieren
Anwendung im Betriebssystem Astra Linux im Modus für abgeschlossene Softwareumgebungen starten
Anwendung im Betriebssystem ALT SP im Modus für geschlossene Softwareumgebungen starten
Betriebssystem OSnova für die Ausführung der Anwendung konfigurieren
Optimierung der Ressourcenauslastung durch die Anwendung
Empfehlungen für typische Serverrollen
Nutzung der Geräteressourcen durch die Anwendung analysieren
Nutzung der Ressourcen durch die Aufgabe zum Schutz vor bedrohlichen Dateien analysieren
Am häufigsten untersuchte Objekte identifizieren
Empfehlungen für den Schutz vor bedrohlichen Dateien und die Untersuchungsaufgaben
Untersuchungsausnahmen konfigurieren
Ausnahmen für das Abfangen von Dateivorgängen konfigurieren
Begrenzung des Speicherverbrauchs der Anwendung festlegen
Empfehlungen für den Schutz vor Web-Bedrohungen und den Schutz vor Netzwerkbedrohungen
Update einer Vorgängerversion der Anwendung durchführen
Informationen zum Aktualisieren der Verwaltungs-Plug-ins für Kaspersky Endpoint Security
Update der Anwendung mithilfe von Kaspersky Security Center durchführen
Update der Anwendung über die Befehlszeile durchführen
Besonderheiten beim Festlegen von Parameterwerten während eines Updates der Anwendung
Anwendung deinstallieren
Informationen zum Deinstallieren der Anwendung und des Administrationsagenten mithilfe von Kaspersky Security Center
Anwendung über die Befehlszeile löschen
Administrationsagent über die Befehlszeile deinstallieren
Deinstallation der Verwaltungs-Plug-ins für Kaspersky Endpoint Security
Lizenzierung der Anwendung
Über den Endbenutzer-Lizenzvertrag
Über die Lizenz
Über das Lizenzzertifikat
Über den Lizenzschlüssel
Über den Aktivierungscode
Über die Schlüsseldatei
Über das Abonnement
Vergleich der Anwendungsfunktionen je nach Lizenz
Anwendung aktivieren und Lizenzschlüssel verwalten
App über Kaspersky Security Center aktivieren
Lizenzschlüsselverwaltung über die Befehlszeile

Informationen zu den verwendeten Lizenzschlüsseln anzeigen
Informationen zu den Schlüsseln auf einem Gerät über die Web Console anzeigen
Informationen zu den Schlüsseln auf einem Gerät über die Verwaltungskonsole anzeigen
Lizenz- und Schlüsselinformationen über die Befehlszeile anzeigen
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 Network Detection and Response (KATA)" bereitgestellt werden
Daten, die bei der Integration mit der Lösung "Kaspersky Unified Monitoring and Analysis Platform" bereitgestellt werden
Konzept der Anwendungsverwaltung
Anwendung mithilfe von Kaspersky Security Center verwalten
Über die Verwaltungs-Plug-ins für Kaspersky Endpoint Security
Über die Richtlinien von Kaspersky Security Center
Über die Aufgaben für Kaspersky Endpoint Security, die in Kaspersky Security Center erstellt wurden
An Web Console und Cloud Console an- und abmelden
Richtlinienverwaltung in der Web Console
Richtlinienerstellung in der Web Console
Richtlinieneinstellungen in der Web Console ändern
Richtlinieneinstellungen in der Web Console
Richtlinien in der Verwaltungskonsole verwalten
Richtlinien mithilfe der Verwaltungskonsole erstellen
Richtlinieneinstellungen in der Kaspersky Security Center Verwaltungskonsole ändern
Richtlinieneinstellungen in der Verwaltungskonsole
Aufgabenverwaltung in der Web Console
Aufgabenerstellung in der Web Console
Aufgabeneinstellungen in der Web Console ändern
Aufgaben in der Web Console starten, beenden, anhalten und fortsetzen
Aufgaben in der Verwaltungskonsole verwalten
Aufgaben in der Verwaltungskonsole erstellen
Aufgabeneinstellungen in der Verwaltungskonsole ändern
Aufgaben in der Verwaltungskonsole starten, beenden, anhalten und fortsetzen
Anwendung über die Befehlszeile verwalten
Aktivieren der automatischen Vervollständigung des kesl-control-Befehls (Bash-Vervollständigung)
Aufgabenverwaltung über die Befehlszeile
Aufgabenliste über die Befehlszeile anzeigen
Aufgabenstatus über die Befehlszeile anzeigen
Aufgabe über die Befehlszeile erstellen

Aufgabe über die Befehlszeile starten, beenden, anhalten und fortsetzen
Aufgabe über die Befehlszeile löschen
Aufgabeneinstellungen über die Befehlszeile ausgeben
Aufgabeneinstellungen über die Befehlszeile bearbeiten
Aufgabeneinstellungen mithilfe einer Konfigurationsdatei bearbeiten
Aufgabeneinstellungen mithilfe der Befehlszeilenschalter bearbeiten
Standardaufgabeneinstellungen über die Befehlszeile wiederherstellen
Aufgabenzeitplan über die Befehlszeile anpassen
Allgemeine App-Einstellungen über die Befehlszeile verwalten
Allgemeine Anwendungseinstellungen ausgeben
Allgemeine Anwendungseinstellungen ändern
Filter zur Eingrenzung der Abfrageergebnisse verwenden
Anwendungseinstellungen exportieren und importieren
Benutzerrollen über die Befehlszeile verwalten
Liste von Benutzern und Rollen anzeigen
Einem Benutzer eine Rolle zuweisen
Einem Benutzer eine Rolle entziehen
Anwendung starten und beenden
Anwendung mithilfe von Web Console starten und beenden
Anwendung mithilfe der Verwaltungskonsole starten und beenden
App über die Befehlszeile starten und beenden
Informationen zum Schutzstatus des Geräts und zur Programmleistung anzeigen
Schutzstatus des Geräts in der Web Console anzeigen
Schutzstatus des Geräts in der Verwaltungskonsole anzeigen
Informationen über die Ausführung der Anwendung in der Web Console anzeigen
Informationen über die Ausführung der Anwendung in der Verwaltungskonsole anzeigen
Informationen über die Ausführung der Anwendung über die Befehlszeile anzeigen
Statistiken zur Ausführung der Anwendung anzeigen
Statistiken zur Ausführung der Anwendung in der Web Console anzeigen
Statistiken zur Ausführung der Anwendung in der Verwaltungskonsole anzeigen
Liste mit Mountpunkten in der Web Console anzeigen
Liste mit Mountpunkten in der Verwaltungskonsole anzeigen
Statistiken zur Ausführung der Anwendung und Liste mit Mountpunkten in der Befehlszeile anzeigen
Kennzahlen zum Systemzustand sammeln
Datenbanken und Module der Anwendung aktualisieren
Informationen zum Aktualisieren von Datenbanken und Modulen
Informationen zu Update-Quellen und -Szenarien
Datenbanken und Module der Anwendung in der Web Console aktualisieren
Datenbanken und Module der Anwendung in der Verwaltungskonsole aktualisieren
Datenbanken und Module der Anwendung über die Befehlszeile aktualisieren
Update mithilfe von Kaspersky Update Utility
Rollback von Datenbanken- und Modul-Updates durchführen
Schutz vor bedrohlichen Dateien
Schutz vor bedrohlichen Dateien in der Web Console konfigurieren
Schutz vor bedrohlichen Dateien in der Verwaltungskonsole konfigurieren
Fenster "Untersuchungsbereiche"
Fenster <Neuer Untersuchungsbereich>

Fenster "Untersuchungseinstellungen"
Fenster "Aktionen beim Erkennen von Bedrohungen"
Ausschlüsse aus dem Schutz vor bedrohlichen Dateien
Fenster "Ausschlussbereiche"
Fenster <Neuer Ausschlussbereich>
Fenster "Ausnahmen nach Maske"
Fenster "Ausschlüsse nach Bedrohungsname"
Fenster "Ausnahmen nach Prozess"
Fenster "Vertrauenswürdiger Prozess"
Schutz vor bedrohlichen Dateien über die Befehlszeile konfigurieren
Einstellungen der Aufgabe zum Schutz vor bedrohlichen Dateien
Optimierung der Überprüfung von Netzwerkverzeichnissen
Besonderheiten der Untersuchung von symbolischen Links und festen Links
Schadsoftware-Untersuchung.
Schadsoftware-Untersuchung in der Web Console
Fenster zum Hinzufügen des Untersuchungsbereichs
Abschnitt "Untersuchungsbereiche"
Fenster "Untersuchungsbereiche"
Abschnitt "Ausschlussbereiche"
Fenster "Ausschlussbereiche"
Fenster zum Hinzufügen des Ausschlussbereichs
Fenster "Ausnahmen nach Maske"
Fenster "Ausschlüsse nach Bedrohungsname"
Schadsoftware-Untersuchung in der Verwaltungskonsole
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"
Schadsoftware-Untersuchung über die Befehlszeile
Einstellungen der vordefinierten Aufgabe zur Schadsoftware-Untersuchung
Benutzerdefinierte Untersuchung von Dateien und Verzeichnissen über die Befehlszeile
Untersuchung wichtiger Bereiche.
Untersuchung wichtiger Bereiche in der Web Console
Fenster zum Hinzufügen des Untersuchungsbereichs
Abschnitt "Untersuchungsbereiche"
Fenster "Untersuchungsbereiche"
Abschnitt "Ausschlussbereiche"
Fenster "Ausschlussbereiche"
Fenster zum Hinzufügen des Ausschlussbereichs

Fenster "Ausnahmen nach Maske"
Fenster "Ausschlüsse nach Bedrohungsname"
Untersuchung wichtiger Bereiche in der Verwaltungskonsole
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 über die Befehlszeile
Untersuchung von Wechseldatenträgern
Untersuchung von Wechseldatenträgern in der Web Console konfigurieren
Untersuchung von Wechseldatenträgern in der Verwaltungskonsole konfigurieren
Untersuchung von Wechseldatenträgern über die Befehlszeile konfigurieren
Container untersuchen
Container-Überwachung
Container-Überwachung in der Web Console konfigurieren
Container-Überwachung in der Verwaltungskonsole konfigurieren
Fenster "Einstellungen der Container-Untersuchung"
Container-Überwachung über die Befehlszeile konfigurieren
Untersuchung von Containern und Images auf Befehl
Untersuchung von Containern in der Web Console
Abschnitt "Ausschlussbereiche"
Fenster "Ausnahmen nach Maske"
Fenster "Ausschlüsse nach Bedrohungsname"
Untersuchung von Containern in der Verwaltungskonsole
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 Containern über die Befehlszeile
Einstellungen der Aufgabe zur Untersuchung von Containern
Benutzerdefinierte Untersuchung von Containern und Images
Integration mit Jenkins
Firewall-Verwaltung
Über Netzwerkpaketregeln
Über dynamische Regeln
Über vorinstallierte verfügbare Netzwerke
Firewall-Verwaltung in der Web Console

- Firewall-Verwaltung in der Verwaltungskonsole
  - Fenster "Regeln für Netzwerkpakete"
  - Fenster "Netzwerkpaketregel hinzufügen"
  - Fenster "IP-Adressen hinzufügen"
  - Fenster "Verfügbare Netzwerke"
  - Fenster "Netzwerkverbindung"
- Firewall-Verwaltung über die Befehlszeile
  - Liste von Regeln für Netzwerkpakete über die Befehlszeile konfigurieren
  - Netzwerkzonen über die Befehlszeile konfigurieren

Schutz vor Web-Bedrohungen
- Schutz vor Web-Bedrohungen in der Web Console konfigurieren
- Schutz vor Web-Bedrohungen in der Verwaltungskonsole konfigurieren
  - Fenster "Vertrauenswürdige Webadressen"
  - Fenster "Untersuchungseinstellungen"
- Schutz vor Web-Bedrohungen über die Befehlszeile konfigurieren

Netzwerkverkehr untersuchen
- Über den Modus zum Abfangen des Datenverkehrs
- Untersuchung des Netzwerkverkehrs in der Web Console konfigurieren
- Untersuchung des Netzwerkverkehrs in der Verwaltungskonsole konfigurieren
  - Fenster "Vertrauenswürdige Domänen"
  - Fenster "Vertrauenswürdige Zertifikate"
  - Fenster "Ausnahmen vom Abfangen des Datenverkehrs"
  - Fenster "Ausnahme vom Abfangen des Datenverkehrs"
  - Fenster "Überwachte Ports"
- Untersuchung des Netzwerkverkehrs über die Befehlszeile konfigurieren
  - 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
- Ausnahmen vom Abfangen des Datenverkehrs durch Tools des Betriebssystems

Schutz vor Netzwerkbedrohungen
- Schutz vor Netzwerkbedrohungen in der Web Console konfigurieren
- Schutz vor Netzwerkbedrohungen in der Verwaltungskonsole konfigurieren
  - Fenster "Ausnahmen"
- Schutz vor Netzwerkbedrohungen über die Befehlszeile konfigurieren

Schutz vor E-Mail-Bedrohungen
- Schutz vor E-Mail-Bedrohungen in der Web Console konfigurieren
- Verwaltungskonsole in der Verwaltungskonsole konfigurieren
  - Fenster "Einstellungen des Schutzes vor E-Mail-Bedrohungen"
  - Fenster "Anhangsfilter"
- Schutz vor E-Mail-Bedrohungen über die Befehlszeile konfigurieren

Schutz vor BadUSB-Angriffen
- Schutz vor BadUSB-Angriffen in der Web Console konfigurieren
- Schutz vor BadUSB-Angriffen in der Verwaltungskonsole konfigurieren
- Schutz vor BadUSB-Angriffen über die Befehlszeile konfigurieren

Schutz vor bösartiger Remote-Verschlüsselung
Schutz vor Verschlüsselung in der Web Console konfigurieren
Schutz vor Verschlüsselung in der Verwaltungskonsole konfigurieren
Fenster "Untersuchungsbereiche"
Fenster „Neuer Untersuchungsbereich“
Fenster "Schutzeinstellungen"
Fenster "Ausschlussbereiche"
Fenster „Neuer Ausnahmebereich“
Fenster "Ausnahmen nach Maske"
Schutz vor Verschlüsselung über die Befehlszeile konfigurieren
Blockierte Geräte verwalten
Programmkontrolle
Über die Regeln für die Programmkontrolle
Testmodus für Regeln der Programmkontrolle
Programmkontrolle in der Web Console konfigurieren
Programmkontrolle in der Verwaltungskonsole konfigurieren
Fenster "Regeln der Programmkontrolle"
Fenster "Regel hinzufügen"
Fenster "Programmkategorien"
Fenster "Benutzer oder Gruppe"
Programmkontrolle über die Befehlszeile konfigurieren
Einstellungen der Aufgabe zur Programmkontrolle
Eine Liste mit Kategorien erstellen und bearbeiten
Eine Liste mit Kategorien anzeigen
Einstellung der Liste mit Regeln für die Programmkontrolle
Parameter der Programmkontrolle exportieren und importieren
Inventarisierung
Inventarisierung in der Web Console konfigurieren
Fenster zum Hinzufügen des Untersuchungsbereichs
Abschnitt "Ausschlussbereiche"
Fenster "Ausschlussbereiche"
Fenster zum Hinzufügen des Ausschlussbereichs
Inventarisierung in der Verwaltungskonsole konfigurieren
Fenster "Untersuchungsbereiche"
Fenster „Neuer Untersuchungsbereich“
Abschnitt "Ausnahmen"
Fenster "Ausschlussbereiche"
Fenster „Neuer Ausnahmebereich“
Inventarisierung über die Befehlszeile konfigurieren
Einstellungen der Inventarisierungsaufgabe
Liste der gefundenen Anwendungen anzeigen
Gerätekontrolle
Gerätekontrolle in der Web Console konfigurieren
Gerätekontrolle in der Verwaltungskonsole konfigurieren
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"
Benachrichtigungsvorlagen der Gerätekontrolle konfigurieren
Gerätekontrolle über die Befehlszeile konfigurieren
Einstellungen der Gerätekontrolle
Liste der verbundenen Geräte in der Befehlszeile anzeigen und exportieren
Liste vertrauenswürdiger Geräte über die Befehlszeile verwalten
Temporären Zugriff auf das Gerät gewähren
Zugriff auf ein Gerät in der Web Console gewähren
Temporären Zugriff auf ein Gerät über die Befehlszeile erhalten
Web-Kontrolle
Über die Zugriffsregeln für Webressourcen
Die Web-Kontrolle in der Web Console konfigurieren
Die Web-Kontrolle in der Verwaltungskonsole konfigurieren
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"
Benachrichtigungsvorlagen der Web-Kontrolle konfigurieren
Die Web-Kontrolle über die Befehlszeile konfigurieren
Einstellungen der Aufgabe "Web-Kontrolle"
Einstellungen der Web-Kontrolle anzeigen und ändern
Regeln zum Definieren von Adressmasken für Webressourcen
Überwachung der System-Integrität
Überwachung der Systemintegrität in Echtzeit
Überwachung der Systemintegrität in der Web Console konfigurieren
Überwachung der Systemintegrität in der Verwaltungskonsole konfigurieren
Fenster "Untersuchungsbereiche"
Fenster „Neuer Untersuchungsbereich“
Fenster "Ausschlussbereiche"
Fenster „Neuer Ausnahmebereich“
Fenster "Ausnahmen nach Maske"
Überwachung der Systemintegrität über die Befehlszeile konfigurieren

- Überwachung der System-Integrität
  - Prüfung der Systemintegrität in der Web Console
    - Fenster zum Hinzufügen des Untersuchungsbereichs
    - Abschnitt "Ausschlussbereiche"
    - Fenster "Ausschlussbereiche"
    - Fenster zum Hinzufügen des Ausschlussbereichs
    - Fenster "Ausnahmen nach Maske"
  - Prüfung der Systemintegrität in der Verwaltungskonsole
    - Fenster "Untersuchungsbereiche"
    - Fenster „Neuer Untersuchungsbereich“
    - Abschnitt "Ausschlussbereiche"
    - Fenster "Ausschlussbereiche"
    - Fenster „Neuer Ausnahmebereich“
    - Fenster "Ausnahmen nach Maske"
  - Prüfung der Systemintegrität über die Befehlszeile konfigurieren
- Verhaltensanalyse
  - Verhaltensanalyse in der Web Console konfigurieren
  - Verhaltensanalyse in der Verwaltungskonsole konfigurieren
    - Fenster "Ausnahmen nach Prozess"
    - Fenster "Vertrauenswürdiger Prozess"
  - Verhaltensanalyse über die Befehlszeile konfigurieren
- Exploit-Prävention
  - Exploit-Prävention in der Web Console konfigurieren
  - Exploit-Prävention in der Verwaltungskonsole konfigurieren
    - Fenster "Ausnahmen aus der Exploit-Prävention"
    - Fenster "Ausnahme aus der Exploit-Prävention"
  - Exploit-Prävention über die Befehlszeile konfigurieren
- Verwendung von Kaspersky Security Network
  - Verwendung von Kaspersky Security Network in der Web Console konfigurieren
  - Verwendung von Kaspersky Security Network in der Verwaltungskonsole konfigurieren
    - Einstellungen für Kaspersky Security Network
    - Erklärung zu Kaspersky Security Network
    - Erklärung zu Kaspersky Private Security Network
  - Verwendung von Kaspersky Security Network über die Befehlszeile konfigurieren
    - Verbindung mit Kaspersky Security Network über die Befehlszeile prüfen
    - Cloud-Modus über die Befehlszeile aktivieren oder deaktivieren
- Erweiterte Einstellungen für die Ausführung der Anwendung
  - Proxyserver konfigurieren
    - Proxyserver-Einstellungen in der Web Console konfigurieren
    - Proxyserver-Einstellungen in der Verwaltungskonsole konfigurieren
      - Fenster "Proxyserver-Ausnahmen"
    - Proxyserver-Einstellungen über die Befehlszeile konfigurieren
  - Globale Ausschlüsse konfigurieren
    - Globale Ausschlüsse in der Web Console konfigurieren
    - Globale Ausschlüsse in der Verwaltungskonsole konfigurieren
      - Fenster "Pfad zum Mountpunkt"
    - Globale Ausnahmen über die Befehlszeile konfigurieren

- Ausschließen des Prozessspeichers von Untersuchungen
- Modus des Interceptors von Dateioperationen auswählen
- Erkennen von Anwendungen konfigurieren, die von Angreifern für Kompromittierungen ausgenutzt werden können
- Überwachung der Anwendungsstabilität aktivieren
- Starteinstellungen der Anwendung konfigurieren
- Begrenzung des von der Anwendung verwendeten residenten Speichers
- Begrenzung der verwendeten Speicher- und CPU-Ressourcen
- Begrenzung der Anzahl der Aufgaben zur benutzerdefinierten Untersuchung
- Übertragung von Informationen an den Speicher von Kaspersky Security Center konfigurieren
- Berechtigungen für die Aufgabenverwaltung konfigurieren
- Ausführung von Aufgaben im Akkubetrieb beenden
- Abfangen von Systemereignissen konfigurieren
  - Möglichkeit zur Installation des aktualisierbaren Kernel-Moduls überprüfen
  - "Abgesicherter" Modus bei Verwendung des aktualisierbaren Kernel-Moduls
  - Einstellungen für das Abfangen in der Web Console konfigurieren
  - Einstellungen für das Abfangen in der Verwaltungskonsole konfigurieren
  - Einstellungen für das Abfangen über die Befehlszeile konfigurieren
- Erweiterte Einstellungen für Telemetriedaten konfigurieren

Datenverwaltung

- Backup-Einstellungen in der Web Console konfigurieren
- Backup-Einstellungen in der Verwaltungskonsole konfigurieren
- Konfigurieren der Backup-Einstellungen über die Befehlszeile
- Verwendung von Objekten im Backup über die Befehlszeile

Integration mit Detection and Response

- Über die Reaktionsmaßnahmen auf Befehle von Detection and Response
- Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise)
  - So bereiten Sie ein Referenzabbild für die korrekte Integration mit EDR Expert (on-premise) vor
  - Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) in der Web Console einrichten
  - Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) über die Befehlszeile einrichten
    - Parameter für die Integration mit Endpoint Detection and Response Expert (on-premise)
    - Zertifikate für die Verbindung mit OSMP-Servern verwalten
- Integration mit Kaspersky Anti Targeted Attack Platform
  - Integration mit Kaspersky Endpoint Detection and Response (KATA) in der Web Console einrichten
  - Integration mit Kaspersky Endpoint Detection and Response (KATA) in der Verwaltungskonsole einrichten
    - Verbindung mit den KATA-Servern konfigurieren
    - Allgemeine Einstellungen für die Verbindung mit KATA-Servern konfigurieren
    - Datenübertragung an die KATA-Server konfigurieren
  - Integration mit Kaspersky Endpoint Detection and Response (KATA) über die Befehlszeile einrichten
    - 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) in der Web Console einrichten
  - Integration mit Kaspersky Network Detection and Response (KATA) in der Verwaltungskonsole einrichten
    - Konfiguration der Verbindung mit NDR-Servern
    - Allgemeine Einstellungen für die Verbindung zu NDR-Servern konfigurieren
    - Konfiguration der Datenübertragung an die NDR-Server

Integration mit Kaspersky Network Detection and Response (KATA) über die Befehlszeile einrichten
Parameter für die Integration mit Kaspersky Network Detection and Response (KATA)
Zertifikate für die Verbindung mit dem NDR-Server verwalten
Integration mit Sandbox
Integration mit Sandbox in Web Console konfigurieren
Integration mit Sandbox über die Befehlszeile konfigurieren
Einstellungen für die Integration mit Sandbox
Verwaltung der Zertifikate für die Verbindung mit dem Sandbox-Server
Integration mit Kaspersky Endpoint Detection and Response Optimum
Integration mit Kaspersky Endpoint Detection and Response Optimum aktivieren und deaktivieren
Integration mit Kaspersky Endpoint Detection and Response Optimum in der Web Console aktivieren und deaktivieren
Integration mit Kaspersky Endpoint Detection and Response Optimum über die Befehlszeile aktivieren und deaktivieren
Status der Integration mit Kaspersky Endpoint Detection and Response Optimum
Informationen zur erkannten Bedrohung und möglichen Reaktionsmaßnahmen anzeigen
Integration von Kaspersky Managed Detection and Response
Empfehlungen zum Erstellen eines Referenzabbilds für die korrekte Integration mit MDR
KPSN-Konfigurationsdatei zur Integration von Kaspersky Managed Detection and Response hochladen
Integration mit Kaspersky Managed Detection and Response in der Web Console konfigurieren
Integration mit Kaspersky Managed Detection and Response in der Verwaltungskonsole konfigurieren
Integration mit Kaspersky Managed Detection and Response über die Befehlszeile konfigurieren
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
Ausnahmen von der Netzwerkisolation im automatischen Modus konfigurieren
Fenster "Ausnahme für die Netzwerkisolation hinzufügen"
Fenster "Liste mit Netzwerkprofilen"
Netzwerkisolation eines Geräts über die Befehlszeile verwalten
Quarantäne verwenden
Dateien mithilfe der Web Console in die Quarantäne verschieben
Quarantäne-Einstellungen in Web Console konfigurieren
Quarantäne-Einstellungen in der Verwaltungskonsole konfigurieren
Quarantäne-Einstellungen über die Befehlszeile konfigurieren
Quarantäne-Dateien über die Befehlszeile verwalten
Einen Prozess starten
Eines Prozesses beenden
Datei von Gerät abrufen
Datei von Gerät löschen
IOC-Untersuchung
Über die Web Console nach Kompromittierungsindikatoren suchen
Über die Befehlszeile nach Kompromittierungsindikatoren suchen
Anforderungen an IOC-Dateien
Ausführungsprävention für Objekte
Ausführungsprävention für Objekte in der Web Console konfigurieren
Ausführungsprävention für Objekte in der Verwaltungskonsole konfigurieren
Ausführungsprävention für Objekte über die Befehlszeile konfigurieren

Cloud Sandbox
Integration mit Kaspersky Unified Monitoring and Analysis Platform
Integration mit KUMA in der Web Console konfigurieren
Integration mit KUMA in der Verwaltungskonsole konfigurieren
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
Integration mit KUMA über die Befehlszeile konfigurieren
Einstellungen der Aufgabe zur Integration mit Kaspersky Unified Monitoring and Analysis Platform
Verwaltung der Zertifikate für die Verbindung mit dem KUMA-Server
Einstellungen zur Verwendung der Anwendung im Light Agent-Modus konfigurieren
Light Agent-Einstellungen in der Web Console konfigurieren
Light Agent-Einstellungen in der Verwaltungskonsole konfigurieren
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
Informationen zur Verwendung der Anwendung im Light Agent-Modus über die Befehlszeile anzeigen
Ereignisse und Berichte anzeigen
Protokollierung von Ereignissen im Protokoll des Betriebssystems konfigurieren
Einstellungen des Ereignisprotokolls der Anwendung konfigurieren
Ereignisse in Kaspersky Security Center anzeigen
Ereignisse über die Befehlszeile anzeigen
Einstellungen für Pop-up-Benachrichtigungen über die grafische Benutzeroberfläche konfigurieren
App über die grafische Benutzeroberfläche verwalten
Grafische Oberfläche
Anwendungskomponenten aktivieren und deaktivieren
Untersuchungsaufgaben starten und beenden
Benutzerdefinierte Untersuchung und Untersuchung in Sandbox starten
Update-Aufgabe starten und beenden
Verwendung von Kaspersky Security Network konfigurieren
Berichte anzeigen
Objekte im Backup anzeigen
Lizenzschlüssel verwalten
Einen Lizenzschlüssel hinzufügen
Einen Lizenzschlüssels entfernen
Lizenz-Info anzeigen
Temporären Zugriff auf ein Gerät erhalten
Informationen über die Anwendung anzeigen
Protokolldatei erstellen
Integritätsprüfung der Anwendungskomponenten

Anfrage an den Technischen Support
Technischer Support über das Kaspersky CompanyAccount
Informationen für den Technischen Support abrufen
Über Protokolldateien der Anwendung
Protokolleinstellungen der Anwendung konfigurieren
Über Protokolldateien der Verwaltungs-Plug-ins für die Anwendung
Über Dump-Dateien
Parameter der Dump-Erstellung konfigurieren
Ferndiagnose von Geräten mithilfe von Kaspersky Security Center
Anwendungen
Anhang 1. Befehle zur Verwaltung von Kaspersky Endpoint Security
Befehle zur Verwaltung der Einstellungen und Aufgaben der App
Befehle zur Verwaltung der allgemeinen Anwendungseinstellungen
Befehle zur Verwaltung der Aufgabeneinstellungen
Befehle zur Aufgabenverwaltung
Befehle zur Verwaltung der Ausführungsprävention für Objekte
Befehle zur Verwaltung der allgemeinen Einstellungen für die Untersuchung von Containern
Befehle zur Verwaltung der Einstellungen für die Untersuchung des Netzwerkverkehrs
Statistikbefehle
Befehle zur Anzeige von Ereignissen
Befehle zur Verwaltung der Ereignisse der Anwendung
Befehle zur Verwaltung der Lizenzschlüssel
Befehle zur Firewall-Verwaltung
Befehle zur Verwaltung blockierter Geräte
Befehle zur Verwaltung der Gerätekontrolle
Befehle zur Verwaltung der Programmkontrolle
Befehle zur Verwaltung der Web-Kontrolle
Befehle zur Backup-Verwaltung
Befehle zur Verwaltung der Quarantäne
Befehle zur Verwaltung von Benutzern und Rollen
Befehle zur Verwaltung von EDR Expert (on-premise)
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
Befehle der Anwendung im Light Agent-Modus zum Schutz virtueller Umgebungen
Befehle zur Verwaltung der Sammlung von Kennzahlen zum Systemzustand
Anhang 2. Konfigurationsdateien und Standardeinstellungen der App
Regeln zum Ändern von Konfigurationsdateien für die Aufgaben der Anwendung
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)
Allgemeine Anwendungseinstellungen
Allgemeine Einstellungen der Untersuchung von Containern
Einstellungen der Untersuchung des Netzwerkdatenverkehrs
Einstellungen des Aufgabenzeitplans
Anhang 3. Rückgabecodes der Befehlszeile
Anhang 4. Einstellungen für die Zusammenarbeit mit Kaspersky Anti-Virus für Linux Mail Server
Anhang 5. Anwendungsparameter in der Richtlinie in der Web Console
Geräteschutz vor Bedrohungen
Schutz vor bedrohlichen Dateien
Schutz vor BadUSB-Angriffen
Untersuchung von Wechseldatenträgern
Verhaltensanalyse
Schutz vor Verschlüsselung
Exploit-Prävention
Schutz von Verbindungen und Kommunikation über das Netzwerk
Schutz vor E-Mail-Bedrohungen
Schutz vor Web-Bedrohungen
Schutz vor Netzwerkbedrohungen
Firewall.
Sicherheitskontrolle
Gerätekontrolle
Web-Kontrolle
Programmkontrolle
Überwachung der System-Integrität
Vertrauenswürdige Zone
Allgemeine Einstellungen
Konfiguration der Erkennung
Kaspersky Security Network
Interaktion mit den Benutzern

Leistung
Netzwerkeinstellungen
Container untersuchen
Technischen Support
Berichte und Speicher
Integration mit KSC
Konfiguration der Kommunikation mit dem Betriebssystem
Ereigniseinstellungen
Telemetrie-Einstellungen
Integrierte Agenten
Managed Detection and Response
Endpoint Detection and Response Optimum
Endpoint Detection and Response Expert (on-premise)
Network Detection and Response (KATA)
Sandbox
Integration mit KUMA
Light Agent-Modus
Einstellungen der SVM-Erkennung
Einstellung der Verbindung mit dem Integrationsserver
Tag für die Verbindung zur SVM
Algorithmus der SVM-Auswahl
Schutz der Verbindung
Anhang 6. Parameter für die Interaktion mit externen Diensten
Interoperabilität mit Kaspersky-Lösungen
Kaspersky Security Center Linux
Network Detection and Response (KATA)
Kaspersky Unified Monitoring and Analysis Platform
Informationsquellen zu Kaspersky Endpoint Security
Glossar
Abonnement
Administrationsgruppe
Administrationsserver
Aktive Richtlinie
Aktiver Schlüssel
Anwendungseinstellungen
App-Datenbanken
Ausnahme
Autostart-Objekte
Dateimaske
Datenbank mit bösartigen Webadressen
Datenbank mit Phishing-Webadressen
Desinfektion von Objekten
Fehlalarm
Gruppenaufgabe
Gruppenrichtlinie
Infiziertes Objekt
Integrationsserver

Kaspersky-Update-Server
Light Agent
Lizenz
Lizenzzertifikat
Programm aktivieren
Proxy-Server
Reserveschlüssel
Richtlinie
Schutz vor Verschlüsselung
SIEM-System
SVM
Vertrauenswürdiges Gerät
Informationen über den Code von Drittherstellern
Markenrechtliche Hinweise

Hilfe von Kaspersky Endpoint Security 12.4 für Linux

Neue Funktionen

Die neuen Funktionen von Kaspersky Endpoint Security 12.4 für Linux

Hardware- und Softwarevoraussetzungen

Hardware- und Softwarevoraussetzungen der Anwendung

Vergleich der Funktionen

- Vergleich der Anwendungsfunktionen je nach Lizenz
- Besonderheiten bei der Verwendung der Anwendung im Light Agent-Modus
- Besonderheiten bei der Verwendung der Anwendung im Modus als Endpoint Detection and Response Agent

Erste Schritte

- Eine Kurzanleitung zur Installation und Erstkonfiguration der Anwendung über die Befehlszeile (Verwendung der Anwendung im Standard-Modus)
- Upgrade einer älteren Programmversion
- Anwendungsinstallation vorbereiten
- Installation und Ersteinrichtung der App
- Datenbanken und Module der Anwendung während der Erstkonfiguration über die Befehlszeile aktualisieren
- Datenbanken und Module der Anwendung über die vordefinierte Update-Aufgabe aktualisieren (nach der Erstkonfiguration)
- Anwendung für die gemeinsame Ausführung mit Kaspersky Security Center vorbereiten

Lizenzverwaltung

- Lizenzierung der Anwendung
- Anwendung aktivieren und Lizenzschlüssel verwalten
- Anwendung während der Erstkonfiguration über die Befehlszeile aktivieren
- Aktivierung der Anwendung und Verwaltung der Lizenzschlüssel über die Kommandozeile (nach der Erstkonfiguration)
- App über Kaspersky Security Center aktivieren

Überwachung und Berichterstattung

- Schutzstatus des Geräts und Informationen zur Ausführung der Anwendung anzeigen
- Informationen über die Ausführung der Anwendung über die Befehlszeile anzeigen
- Ereignisse und Berichte anzeigen

Bereitstellung von Daten und Schutz personenbezogener Daten

- Bereitstellung von Daten

Weitere Funktionen

- Einstellungen zur Verwendung der Anwendung im Light Agent-Modus konfigurieren
- Erweiterte Einstellungen für die Ausführung der Anwendung konfigurieren
- Verwendung von Kaspersky Security Network
- Backup
- Integration mit Detection and Response

Optimierung des Ressourcenauslastung des Betriebssystems

- Optimierung der Ressourcenauslastung

Kontaktaufnahme mit dem Technischen Support

- Grundlegende Schritte zur Diagnose von Problemen mit der Anwendung
- Kontaktaufnahme mit dem Technischen Support

Über Kaspersky Endpoint Security 12.4 für Linux

Kaspersky Endpoint Security 12.4 für Linux (im Folgenden auch als „Kaspersky Endpoint Security“ oder „Programm“ bezeichnet) dient dem Schutz von Geräten mit Linux®-Betriebssystemen vor verschiedenen Arten von Bedrohungen, darunter Netzwerkangriffe und betrügerische Angriffe.

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

Die 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.

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

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

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

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

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

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

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

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

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

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

- **Schutz vor E-Mail-Bedrohungen**. Die Komponente *Schutz vor E-Mail-Bedrohungen* untersucht ein- und ausgehende E-Mail-Anhänge auf Viren und andere Bedrohungen.

- **Schutz vor BadUSB-Angriffen**. Die Komponente *Schutz vor BadUSB-Angriffen* verhindert, dass sich infizierte USB-Geräte mit Ihrem Computer verbinden und sich als Tastatur ausgeben.

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

- **Gerätekontrolle**. Mit der Komponente *Gerätekontrolle* können Sie den Benutzerzugriff auf zusätzliche oder externe Geräte verwalten, die auf dem Client-Gerät installiert oder daran angeschlossen sind (z. B. Festplatten, Kameras oder WLAN-Module). Auf diese Weise können Sie das Client-Gerät vor einer Infektion schützen, wenn Sie externe Geräte anschließen, und Datenverlust oder Datenlecks verhindern. Der Benutzerzugriff auf Geräte wird mithilfe des Zugriffsmodus und der von Ihnen konfigurierten Zugriffsregeln überwacht.

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

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

- **Web-Kontrolle**. Die Komponente *Web-Kontrolle* steuert den Benutzerzugriff 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.

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

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

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

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

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

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

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

Kaspersky Endpoint Security kann im informativen Modus ausgeführt werden. *Modus „Nur benachrichtigen"* ist ein Betriebsmodus des Programms, in dem die Programmkomponenten und Aufgaben bei Erkennung einer Bedrohung nicht versuchen, schädliche Objekte zu desinfizieren oder zu löschen, den Zugriff zu verweigern oder die Aktivität von Programmen zu blockieren. Stattdessen informiert das Programm den Benutzer nur über die erkannte Bedrohung.

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

- Die Integration mit Kaspersky Managed Detection and Response gewährleistet die kontinuierliche Suche, Erkennung und Beseitigung von Bedrohungen, die gegen Ihr Unternehmen gerichtet sind.
- Die Integration mit Kaspersky Anti Targeted Attack Platform gewährleistet den Schutz der IT-Infrastruktur des Unternehmens sowie die rechtzeitige Erkennung von Zero-Day-Bedrohungen, gezielten Angriffen und Advanced Persistent Threats.
- Die Integration mit Kaspersky Endpoint Detection and Response Optimum 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.
- Die Integration mit Kaspersky Unified Monitoring and Analysis Platform gewährleistet das Empfangen, Verarbeiten und Speichern von Ereignissen mit Bezug auf die Informationssicherheit. Es bietet die Analyse und Korrelation von Daten, eine Suche nach Ereignissen und die Erstellung von Benachrichtigungen bei erkannten Anzeichen von Bedrohungen der Informationssicherheit.
- Die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) bietet Schutz vor den meisten Cyberrisiken und deckt wichtige Bedrohungsszenarien ab.

Um die Anwendung auf dem neuesten Stand zu halten, werden zusätzliche Anwendungsfunktionen bereitgestellt:

- Aktivierung der Anwendung mithilfe einer Schlüsseldatei oder eines Aktivierungscodes.

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

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

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

- Differenzierung des Benutzerzugriffs auf Funktionen der Anwendung entsprechend den Benutzerrollen.

- Benachrichtigung des Administrators über Ereignisse, die während der Ausführung der Anwendung aufgetreten sind.

- Integritätsprüfung der Anwendungskomponenten mit dem Tool zur Integritätsprüfung.

Kaspersky Endpoint Security kann auf folgende Arten verwaltet werden:

- Mithilfe von Kaspersky Security Center über die Kaspersky Security Center Web Console, die Kaspersky Security Center Cloud Console oder die Verwaltungskonsole.

- Über die Befehlszeile mithilfe von Verwaltungsbefehlen.

- Über die grafische Benutzeroberfläche.

  Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, muss die Anwendung mittels Kaspersky Security Center verwaltet werden. Die Anwendung kann weder über die Kaspersky Security Center Cloud Console noch über die grafische Benutzeroberfläche verwaltet werden.

Die Anwendungsfunktionalitäten für die Aktualisierung (einschließlich Updates des Anti-Virus-Signaturen und der Codebase) und für KSN sind in den USA möglicherweise nicht verfügbar.

Über die Nutzungsmodi von Kaspersky Endpoint Security

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

- Im Standard-Modus zum Schutz von Workstations und Server (im Weiteren auch "Standard-Modus"). Kaspersky Endpoint Security wird als autonome Anwendung zum Schutz von Geräten mit Linux-Betriebssystemen verwendet.
- Im Light Agent-Modus zum Schutz virtueller Umgebungen als Teil von Kaspersky Security for Virtualization Light Agent („Light Agent-Modus“). Kaspersky Endpoint Security wird als Light Agent-Komponente von Kaspersky Security for Virtualization Light Agent für den Schutz von virtuellen Maschinen mit Linux-Gastbetriebssystemen verwendet.
- Im Modus als Endpoint Detection and Response Agent zur gemeinsamen Verwendung der Detection and Response-Lösungen von Kaspersky und der Anti-Virus-Anwendungen von Drittherstellern (im Weiteren auch "Modus als Endpoint Detection and Response Agent") auf geschützten Maschinen.

Die Anwendung kann jeweils nur in einem Modus verwendet werden.

Standardmäßig wird die Anwendung im Standard-Modus verwendet.

Anwendung im Light Agent-Modus verwenden

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

1. Führen Sie die Installation von Kaspersky Endpoint Security im Light Agent-Modus auf jeder virtuellen Maschine durch, die mit Kaspersky Security for Virtualization Light Agent geschützt werden soll. Sie können die Anwendung auch auf einer Vorlage für virtuelle Maschinen installieren.

   Bevor Sie mit der Installation der Anwendung beginnen, müssen Sie auf der virtuellen Maschine und den Vorlagen für virtuelle Maschinen den Kaspersky Security Center Administrationsagenten installieren.

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

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

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

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

- Die Rolle der virtuellen Maschine, die Sie in der virtuellen Infrastruktur schützen möchten: Server oder Workstation. Die Rolle der virtuellen Maschine legt fest, unter welcher Lizenz die Anwendung auf dieser virtuellen Maschine verwendet wird und wie groß der verfügbare Funktionsumfang ist.

- Modus zum Schutz der VDI-Infrastruktur Es wird empfohlen, diesen Modus zu aktivieren, wenn Sie die Anwendung auf einer Vorlage für virtuelle Maschinen installieren, aus dem temporäre virtuelle Maschinen erstellt werden. Der Modus zum Schutz der VDI-Infrastruktur optimiert die Ausführung von Kaspersky Endpoint Security auf temporären virtuellen Maschinen.

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

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

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

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

Die Informationen über die Ausführungseinstellungen der Anwendung im Light Agent-Modus und über die Verbindungen zum Integrationsserver und zur SVM können Sie mit dem folgenden Anwendungsbefehlen abrufen:

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

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

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

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

- Der *Ausführungsstatus* gibt an, dass die Anwendung im Light Agent-Modus verwendet wird.

- Der Status *Nicht eingerichtet* gibt an, dass die Anwendung im Standard-Modus oder im Modus als Endpoint Detection and Response Agent ausgeführt wird.

Informationen zum Aktivieren der Anwendung im Light Agent-Modus

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

Möglicherweise sind in der Hauptlizenz von Kaspersky Security for Virtualization Light Agent die erweiterten Funktionen der Anwendung "Kaspersky Endpoint Security" nicht enthalten (z. B. die Integration mit den Detection and Response-Lösungen von Kaspersky). In diesem Fall müssen Sie der SVM einen weiteren Lizenzschlüssel hinzufügen, um die erforderlichen zusätzlichen Funktionen zu aktivieren.

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

Sie können Informationen zu der Lizenz, unter der Light Agent for Linux verwendet wird, entweder remote über Kaspersky Security Center oder direkt auf einer geschützten virtuellen Maschine mit Light Agent über die Befehlszeile anzeigen.

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

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

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

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

Andere Update-Quellen als Ordner auf SVMs werden nicht unterstützt. Die Verwendung von Gruppen-Update-Aufgaben wird nicht unterstützt.

Das Rollback des letzten Updates für Malware-Datenbanken wird ebenfalls auf der Seite des Schutzservers durchgeführt. Nach dem Rollback eines Updates der Datenbanken und Programm-Module auf der SVM wird auf der geschützten virtuellen Maschine eine spezielle lokale Aufgabe vom Typ *Update* gestartet. Dadurch kehrt der Light Agent zur Verwendung der vorherigen Auswahl der Malware-Datenbanken zurück.

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

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

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

- Kann die App 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.

Anwendung im Modus als Endpoint Detection and Response Agent verwenden

Die Anwendung "Kaspersky Endpoint Security" ermöglicht Ihnen im Modus als Endpoint Detection and Response Agent, die Funktionen der Detection and Response-Lösungen von Kaspersky zu nutzen, um Geräte mit installierten Anti-Virus-Anwendungen von Drittanbietern zu schützen.

Im Modus als Endpoint Detection and Response Agent werden die standardmäßigen Schutz- und Kontrollkomponenten von Kaspersky Endpoint Security nicht zum Schutz des Geräts verwendet. Der standardmäßige Schutz des Geräts wird durch eine Anti-Virus-Anwendung eines Drittanbieters gewährleistet. Die Anwendung "Kaspersky Endpoint Security" überwacht im Modus als Endpoint Detection and Response Agent kontinuierlich die auf dem Gerät laufenden Prozesse, offenen Netzwerkverbindungen und geänderten Dateien, und gewährleistet die Integration mit den Detection and Response-Lösungen.

- Kaspersky Endpoint Detection and Response Expert (on-premise), basierend auf der Open Single Management Platform (im Weiteren auch "OSMP").
- Komponenten von Kaspersky Endpoint Detection and Response und Kaspersky Network Detection and Response, die auf der Kaspersky Anti Targeted Attack Platform basieren (im Weiteren auch "KATA").

Kaspersky Endpoint Security 12.4 für Linux kann mit dem Anti-Virus-Programm Dr. Web zusammenarbeiten. Sie können Kaspersky Endpoint Security im Endpoint Detection and Response Agent-Modus auf einem Gerät mit dem Anti-Virus-Programm Dr. Web installieren.

Die Anwendungen sollten in der folgenden Reihenfolge installiert werden: zuerst die Anti-Virus-Anwendung eines Drittanbieters, danach den Kaspersky Security Center Administrationsagenten und anschließend Kaspersky Endpoint Security im Modus als Endpoint Detection and Response Agent. Dies liegt daran, dass der Installer einer Drittanbieteranwendung die Anwendungen von Kaspersky als inkompatible Software erkennen und entfernen kann. Wenn auf einem Gerät eine Drittanbieteranwendung aktualisiert wurde, empfehlen wir, die Funktionalität von Kaspersky Endpoint Security und vom Administrationsagenten zu überprüfen, da der Installer der Drittanbieteranwendung das Gerät erneut auf inkompatible Software überprüft und möglicherweise Anwendungen von Kaspersky entfernt.

Konfiguration der Anwendung im Modus als Endpoint Detection and Response Agent

Wenn Sie die Anwendung "Kaspersky Endpoint Security" im Modus als Endpoint Detection and Response Agent verwenden möchten, müssen Sie die folgenden Schritte ausführen:

1. Führen Sie die Installation der Anwendung "Kaspersky Endpoint Security" im Modus als Endpoint Detection and Response Agent auf jeder zu schützenden virtuellen Maschine durch.

   Informationen über den Nutzungsmodus der Anwendung können Sie über die Befehlszeile mit dem Befehl `kesl-control --app-info` ausgeben.

2. Anwendung aktivieren. Sie müssen der Anwendung einen separaten Lizenzschlüssel hinzufügen: „Kaspersky Endpoint Detection and Response Expert (on-premise) Add-on“ (im Folgenden auch „EDR Expert (on-premise)-Schlüssel“ genannt).

   > Zur Aktivierung der Anwendung im Modus als Endpoint Detection and Response Agent benötigen Sie lediglich einen Schlüssel für die zusätzlichen Funktionen. Es muss kein Haupt-Lizenzschlüssel zur Anwendung hinzugefügt werden.

3. Aktivieren Sie die Integration mit den erforderlichen Detection and Response-Lösungen zum Schutz des Geräts:

   - Für die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) auf der OSMP-Plattform müssen Sie die Komponente EDR Expert (on-premise) aktivieren und die Integrationseinstellungen in der Kaspersky Security Center Web Console oder über die Befehlszeile verwalten.

   - Für die Integration mit Kaspersky Endpoint Detection and Response auf der Plattform Kaspersky Anti Targeted Attack Platform müssen Sie die Komponente EDR Expert (on-premise) aktivieren und die Integrationseinstellungen in der Kaspersky Security Center Web Console, in der Verwaltungskonsole oder über die Befehlszeile verwalten.

   - Um Kaspersky Network Detection and Response (NDR) auf der Kaspersky Anti Targeted Attack Platform zu integrieren, müssen Sie die Komponente "NDR (KATA)" aktivieren und die Integrationseinstellungen in der Kaspersky Security Center Web Console, in der Verwaltungskonsole oder über die Befehlszeile konfigurieren.

   Sie können den Ausführungsstatus der Komponenten EDR Expert (on-premise) und NDR (KATA) wie folgt überprüfen:

   - In den Eigenschaften der Web Console (**Assets (Geräte)** → **Verwaltete Geräte** → Link <Name des Geräts> → **Anwendungen** → Link <Name von Kaspersky Endpoint Security> → **Allgemein** → **Komponenten**).

   - In der Befehlszeile durch Ausführen des folgenden Befehls: `kesl-control --app-info`.

Besonderheiten bei der Verwendung der Anwendung im Modus als Endpoint Detection and Response Agent

Wenn die Anwendung "Kaspersky Endpoint Security" im Modus als Endpoint Detection and Response Agent verwendet wird, sind weniger Komponenten und Aufgaben verfügbar. Nach der Installation werden die Anwendungseinstellungen wie folgt konfiguriert:

- Vollständig konfigurierbare Komponenten, welche die Integration mit den Detection and Response gewährleisten:
  - EDR Expert (on-premise)
  - NDR (KATA)

  Die Komponenten sind standardmäßig deaktiviert. Um die Anwendung im Modus als Endpoint Detection and Response Agent auszuführen, müssen Sie diese aktivieren. 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. Dieser Parameter kann nicht geändert werden.
- 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 Parameter können nicht geändert werden:
  - 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 mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA) kann Kaspersky Endpoint Security im Rahmen einer Aktion zur Reaktion auf Bedrohungen den Start von ausführbaren Dateien und Skripten 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.

Lieferumfang

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

Der Lieferumfang von Kaspersky Endpoint Security umfasst die folgenden Dateien:

- kesl-12.4.0-<Build-Nummer>.i386.rpm, kesl_12.4.0-<Build-Nummer>_i386.deb

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

- kesl-12.4.0-<Build-Nummer>.x86_64.rpm, kesl_12.4.0-<Build-Nummer>_amd64.deb

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

- kesl-12.4.0-<Build-Nummer>.aarch64.rpm, kesl_12.4.0-<Build-Nummer>_arm64.deb

  Diese enthalten die Hauptdateien der App. Pakete für den jeweiligen Paketmanager können auf 64-Bit-Betriebssystemen für die Arm®-Architektur installiert werden.

- kesl-gui-12.4.0-<Build-Nummer>.i386.rpm, kesl-gui_12.4.0-<Build-Nummer>_i386.deb

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

- kesl-gui-12.4.0-<Build-Nummer>.x86_64.rpm, kesl-gui_12.4.0-<Build-Nummer>_amd64.deb

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

- kesl-gui-12.4.0-<Build-Nummer>.aarch64.rpm, kesl-gui_12.4.0-<Build-Nummer>_arm64.deb

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

- kesl-12.4.0.<Build-Nummer>.zip

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

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

- ksn_license.<ID der Sprache>

  Enthält den Text der Erklärung zu Kaspersky Security Network.

- license.<ID der Sprache>

  Enthält den Text des Endbenutzer-Lizenzvertrags. Der Endbenutzer-Lizenzvertrag legt die Bedingungen für die Nutzung des Programms fest.

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.

Hard- und Softwarevoraussetzungen

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

Hardwarevoraussetzungen

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

Hardware-Mindestanforderungen

- Ein Prozessor mit AMD64-Architektur, 2 GHz oder höher, mit mindestens zwei Kernen und Unterstützung für SSE2-Befehle.
- Mindestens 1 GB für die Swap-Partition.
- 2 GB RAM, welcher der Anwendung unter 64-Bit-Betriebssystemen zur Verfügung steht (1 GB RAM bei 32-Bit-Betriebssystemen).
- 4 GB freier Speicher auf der Festplatte für die Installation der App 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.

- Bei Verwendung der grafischen Oberfläche muss der Monitor die Fenster in einer Breite von 1000 Pixeln und einer Höhe von 600 Pixeln darstellen können (bei angewandter Bildschirmskalierung werden diese Abmessungen ebenfalls skaliert).
- Bei Verwendung von Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen wird eine virtuelle Netzwerkschnittstelle mit einer Bandbreite von 100 Mbit/s benötigt.

Minimale Hardwarevoraussetzungen für die Arm-Architektur

- Prozessor Armv8.2-A Kunpeng 920 oder Armv8-A Baikal-M (BE-M1000) oder m-Trust Terminal
- Mindestens 1 GB für die Swap-Partition.
- 2 GB RAM, 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.
- Bei Verwendung der grafischen Oberfläche muss der Monitor die Fenster in einer Breite von 1000 Pixeln und einer Höhe von 600 Pixeln darstellen können (bei angewandter Bildschirmskalierung werden diese Abmessungen ebenfalls skaliert).

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

Softwarevoraussetzungen

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

- 32-Bit-Betriebssysteme:
  - Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12

- 64-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)
  - Astra Linux Special Edition RUSB.10015-01 (operational Update 1.6)
  - Astra Linux Special Edition RUSB.10015-01 (operational Update 1.7)
  - Astra Linux Special Edition RUSB.10015-01 (operational Update 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).

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

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

- CentOS 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
- CentOS Stream 8
- CentOS Stream 9
- CentOS Stream 10
- Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12
- Debian GNU/Linux 13.0, 13.1, 13.2
- 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
- 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
- SberOS 3.4.0, 3.5.0
- SUSE Linux Enterprise Server 12.5, 12.6, 12.7
- SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7
- Ubuntu® 22.04 LTS.
- Ubuntu 24.04 LTS
- ALT Education 10
- ALT Education 11
- ALT Workstation 11
- ALT Server 11
- ALT SP Workstation Release 10
- ALT SP Server Version 10
- Atlant, Build Alcyone, Version 2022.02
- GosLinux 7.2.

- M OS 12 Server Release 2021.1.
- Mos OS 15.5 Arbat
- MSVSphere 9.4 ARM
- MSVSphere 9.4 Server
- OS MESH 12 für alle Anwender (ohne Telemetrie und DIT-Unterstützung) Release 2021.1
- OS MESH 12 für Moskauer Schulen – Version für interaktive Tafeln (mit Telemetrie und DIT-Unterstützung) Release 2021.1
- OS MESH 12 für Moskauer Schulen - Computer und Laptops (mit Telemetrie und DIT-Unterstützung) Release 2021.1
- OSnova 2.14
- OSnova 3.0.5
- 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
- SintezM-Client 8.6
- SintezM-Server 8.6

- 64-Bit-Betriebssysteme für die ARM-Architektur:
  - Astra Linux Special Edition RUSB.10152-02 (reguläres Update 4.7).
  - CentOS Stream 9
  - EulerOS 2.0 SP10
  - SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7
  - Ubuntu 22.04 LTS
  - ALT SP Workstation Release 10
  - ALT SP Server Release 10
  - RED OS 8.0

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

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

Zusätzliche Software-Anforderungen 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 6.4 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.

Für virtuelle Maschinen, auf denen Kaspersky Endpoint Security im Light Agent-Modus installiert werden soll, gelten die Hard- und Software-Anforderungen von Kaspersky Endpoint Security mit den folgenden Einschränkungen.

Das BIOS der geschützten virtuellen Maschine sollte die SMBIOS-Spezifikation in Version 2.1 oder höher unterstützen.

Auf den zu schützenden virtuellen Maschinen sollten die folgenden Pakete in Abhängigkeit von der virtuellen Infrastruktur, in der Kaspersky Security for Virtualization Light Agent bereitgestellt wird, installiert sein:

- In einer Microsoft Hyper-V-Infrastruktur muss auf virtuellen Maschinen das Paket des Integrationsdienstes (Integration Services) installiert sein.
- In einer VMware vSphere-Infrastruktur müssen auf virtuellen Maschinen die VMware Tools installiert sein.
- In einer XenServer-Infrastruktur müssen auf virtuellen Maschinen die XenTools installiert sein.
- In einer HUAWEI FusionSphere-Infrastruktur müssen auf virtuellen Maschinen die HUAWEI Tools installiert sein.
- In einer Infrastruktur von KVM, OpenStack, Private Cloud von VK, TIONICS Cloud Platform, Astra Linux und ALT Virtualization Server, Basis.DynamiX und Basis DynamiX Standard muss auf virtuellen Maschinen der QEMU Guest Agent installiert sein.

Unterstützte Versionen von Kaspersky Security Center

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

- Kaspersky Security Center Windows 14, 14.2, 15.1. Kaspersky Endpoint Security kann über die Verwaltungskonsole mithilfe des MMC-Verwaltungs-Plug-ins und über die Kaspersky Security Center Web Console mithilfe des Web-Verwaltungs-Plug-ins verwaltet werden.

- Kaspersky Security Center Linux 15.1, 15.2, 15.3, 15.4, 16.0, 16.1, 16.2. Das Administrations-Web-Plug-in kann zur Verwaltung von Kaspersky Endpoint Security über die Kaspersky Security Center Web Console verwendet werden.

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

- Kaspersky Security Center Windows 14.2, 15.1.

- Kaspersky Security Center 15.4, 16.0, 16.1, 16.2.

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

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

Wenn Sie die Anwendung in die Kaspersky Endpoint Detection and Response-Komponente der Kaspersky Anti Targeted Attack Platform integrieren, empfehlen wir die Verwendung der folgenden Versionen des Kaspersky Security Center zur Verwaltung der Anwendung:

- Kaspersky Security Center Windows 14.2, 15.1.

- Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2.

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

- Kaspersky Security Center Windows 15.1.

- Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2.

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

Kaspersky Endpoint Security unterstützt die Versionen folgender Lösungen auf Basis der Kaspersky Anti Targeted Attack Platform:

- Kaspersky Anti Targeted Attack Platform 6.0 (Kaspersky Endpoint Detection and Response (KATA) und Kaspersky Network Detection and Response (KATA) und Sandbox).
- Kaspersky Anti Targeted Attack Platform 6.1 (Kaspersky Endpoint Detection and Response (KATA) und Kaspersky Network Detection and Response (KATA) und Sandbox).
- Kaspersky Anti Targeted Attack Platform 7.0 (Kaspersky Endpoint Detection and Response (KATA) und Kaspersky Network Detection and Response (KATA) und Sandbox).
- Kaspersky Anti Targeted Attack Platform 7.1 (Kaspersky Endpoint Detection and Response (KATA) und Kaspersky Network Detection and Response (KATA) und Sandbox).
- Kaspersky Anti Targeted Attack Platform 8.0 (Kaspersky Network Detection and Response (KATA) und Sandbox).

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

Kaspersky Endpoint Security ist kompatibel mit der Lösung Kaspersky Endpoint Detection and Response Expert (on-premise) 8.0 auf Basis der Open Single Management Platform (im Weiteren auch "OSMP").

Weitere Informationen zu Kaspersky Endpoint Detection and Response Expert (on-premise) 8.0 finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premise).

Neuerungen

Kaspersky Endpoint Security bietet jetzt die folgenden Möglichkeiten 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)", welche die Integration mit Kaspersky Endpoint Detection and Response (KATA) gewährleistet, wurde in EDR Expert (OSMP) umbenannt. Diese Komponente stellt außerdem die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) bereit. Die Integrationsaufgabe wurde in *Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise)* (KATAEDR, ID: 24) umbenannt.
- Die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) wurde implementiert. Dies ist eine Cybersecurity-Lösung, die Unternehmen Schutz vor vielfältigen Cyberrisiken bietet und wichtigsten Bedrohungsszenarien abdeckt. 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-premise) 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 (OSMP), welche die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) und mit Kaspersky Endpoint Detection and Response (KATA) gewährleistet, durch das Hinzufügen eines Lizenzschlüssels.

  - Auswählen des Integrationsmodus in den Parametern der Aufgabe zur *Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise)* in der Befehlszeile oder in den Richtlinieneigenschaften 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 Richtlinienabschnitte wurde geändert, um erforderliche Funktionen schneller zu finden.

- Es kann jetzt der von der Anwendung genutzte Modus zum Abfangen des Datenverkehrs ausgewählt werden: Es kann entweder die eBPF-Technologie oder das Tool iptables verwendet werden.

- 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.

- Es können jetzt Richtlinien für mobile Benutzer sowohl in der Web Console als auch in der Verwaltungskonsole erstellt werden. 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 oder beim Anzeigen dieser Liste über die Befehlszeile werden jetzt auch Informationen darüber angezeigt, ob der Mountpunkt in einem Namespace gefunden wurde.

- 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
- Die Liste der unterstützten Betriebssysteme wurde 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 im Web-Plug-in 12.4.0.8289 behobenen Probleme

ID (Kennung)	Description
10724878	Beim Anwenden der Richtlinie auf das Gerät wurde für die Konfiguration `InterceptorApplyStrategy` der Wert `RestartServiceManually` anstelle des Standardwerts `RestartServiceAutomatically` verwendet.

Vorbereitung der Installation von Kaspersky Endpoint Security

Allgemeine Maßnahmen

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

- Überprüfen Sie, ob Ihr Gerät die Hardware- und Softwareanforderungen der Anwendung erfüllt.
- Stellen Sie sicher, dass auf Ihrem Gerät keine Antivirensoftware von Drittanbietern installiert ist.
- Stellen Sie sicher, dass Kaspersky Endpoint Agent für Linux nicht auf Ihrem Gerät installiert ist. Wenn Kaspersky Endpoint Agent für Linux installiert ist, erscheint während der Installation eine Meldung, in der Sie aufgefordert werden, es manuell zu deinstallieren.
- Wenn Sie Kaspersky Endpoint Security mittels Kaspersky Security Center verwalten möchten, führen Sie vorbereitende Schritte aus, um den Kaspersky Security Center Administrationsagenten auf dem Gerät zu installieren (weitere Informationen dazu finden Sie in der Hilfe zu Kaspersky Security Center).

  > Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, muss die Anwendung mittels Kaspersky Security Center verwaltet werden.

- Wenn Sie das System zur Zugriffskontrolle von SELinux verwenden möchten, müssen Sie sicherstellen, dass das Tool "semanage" im Betriebssystem installiert ist. Wenn das Tool nicht installiert ist, installieren Sie je nach Typ des Paketmanagers das Paket policycoreutils-python oder policycoreutils-python-utils.
- Wenn Sie die grafische Benutzeroberfläche verwenden möchten, müssen Sie sicherstellen, dass auf Ihrem Geräte die erforderlichen Abhängigkeiten zur Installation der grafischen Benutzeroberfläche erfüllt werden. Wenn Sich das Gerät in einer geschossenen Netzwerkumgebung befindet und keinen Zugriff auf Repositorys oder Paketverwaltungen hat, wird es empfohlen, die Liste der Abhängigkeiten auf einem Referenzgerät zu überprüfen (libice6, libsm6, libx11-6, libx11-xcb1, libxcb-icccm4, libxcb-image0, libxcb-keysyms1, libxcb-randr0, libxcb-render-util0, libxcb-render0, libxcb-shape0, libxcb-shm0, libxcb-sync1, libxcb-xfixes0, libxcb-xinerama0, libxcb-xkb1, libxcb1, libxi6, libxml2, zlib1g) und anschließend alle Pakete herunterzuladen auf allen Geräten zu verteilen, bevor Sie die Installation über die grafische Benutzeroberfläche durchführen.
- Wenn Sie die grafische Benutzeroberfläche verwenden möchten, müssen Sie sicherstellen, dass das Dienstprogramm Zenity im Betriebssystem installiert ist.
- Stellen Sie auf Geräten mit Betriebssystemen ohne Unterstützung der Fanotify-Technologie sicher, dass Folgendes installiert ist:
  - Pakete zur Programmkompilierung und Aufgabenausführung (gcc, binutils, glibc, glibc-devel, make, ld, rpcbind).
  - Paket mit Kernel-Header-Dateien des Betriebssystems zum Kompilieren der Module von Kaspersky Endpoint Security
- Auf einem Gerät mir dem Betriebssystem SUSE Linux Enterprise Server 15 das Paket "insserv-compat".

- 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**).

  Sie können die ptrace-Ablaufverfolgung deaktivieren, indem Sie das Kernel-Parameter-Wert-Paar `kernel.yama.ptrace_scope=3` angeben. Anschließend ändert sich Anwendungsausführung wie folgt:

  - Bei einem Anwendungsabsturz ist es nicht möglich, eine Dump-Datei des kesl-Prozesses zu erstellen.
  - Die Komponente "Verhaltensanalyse" kann von der Prozessumgebung keine Parameter abrufen.
  - Auf Betriebssystemen mit Kernel-Versionen höher als 5.7 kann die Komponente "Programmkontrolle" keine Befehlszeilenargumente lesen und Umgebungsvariablen verarbeiten, da das Lesen von "/proc/pid/syscall" und "/proc/pid/mem" verboten ist. Auf Betriebssystemen mit Kernel-Version 5.0 funktioniert die Komponente "Programmkontrolle" nicht ordnungsgemäß.
  - In Untersuchungsaufgaben funktioniert die Untersuchung des Prozess- und Kernelspeichers nicht, da das Lesen von "/proc/pid/mem" verboten ist.
  - Im Modus der obligatorischen Zugriffskontrolle kann die YARA-Untersuchung des Prozessspeichers nicht gewährleistet werden, da das Lesen von /proc/pid/mem verboten ist.

- Damit die Komponenten Firewall-Verwaltung, Schutz vor Web-Bedrohungen und Schutz vor Netzwerkbedrohungen funktionieren, müssen Sie das Tool "iptables" auf Ihrem Gerät installieren.

- Damit das MMC-Verwaltungs-Plug-in für Kaspersky Endpoint Security funktioniert, muss auf dem Gerät, auf dem der Kaspersky Security Center Administrationsserver installiert ist, Microsoft® Visual C++® 2015 Redistributable Update 3 RC (siehe https://www.microsoft.com/de-de/download/details.aspx?id=52685) installiert sein.

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

- Vergewissern Sie sich, dass im Betriebssystem die vom Hersteller des Betriebssystems empfohlene Obergrenze für Dateideskriptoren konfiguriert sind. Führen Sie zum Überprüfen des Limits den Befehl `cat /proc/sys/fs/file-max` aus. Während die App ausgeführt wird, kann das Betriebssystem deutlich mehr Deskriptoren verwenden. Im Allgemeinen wird es empfohlen, die Obergrenze für die Anzahl an Dateien, zu deaktivieren, indem Sie in der Datei "/etc/sysctl.conf" den folgenden Parameterwert angeben: `fs.file-max=9223372036854775807`. Nachdem dem Ändern des Parameterwertes muss das Betriebssystem neu gestartet werden.

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

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

- Stellen Sie sicher, dass die zu schützenden virtuellen Maschinen die allgemeinen Anforderungen des Light Agent-Modus erfüllen.

- 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.

Installation und Erstkonfiguration von Kaspersky Endpoint Security

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

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

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

Standard-Modus

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

1. **Installation und Erstkonfiguration des Administrationsagenten**

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

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

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

   - Mit dem webbasierten Verwaltungs-Plug-in für Kaspersky Endpoint Security lässt sich 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.

   - Mit dem MMC-Verwaltungs-Plug-in von Kaspersky Endpoint Security können Sie das Programm über die Kaspersky Security Center Verwaltungskonsole verwalten. Das MMC-Plug-in muss auf dem Gerät installiert werden, auf dem die Kaspersky Security Center Verwaltungskonsole installiert ist.

3. **Anwendungspakete und grafische Benutzeroberfläche installieren**

   Kaspersky Endpoint Security wird in den Paket-Formaten DEB und RPM bereitgestellt. Es sind spezielle Pakete für die Anwendung und deren grafische Oberfläche vorgesehen. Installieren Sie Kaspersky Endpoint Security und bei Bedarf die grafische Oberfläche aus den Paketen des erforderlichen Formats.

   Sie können die Installation auf eine der folgenden Arten durchführen:

   - Über Kaspersky Security Center.

   - Über die Befehlszeile.

4. **Erstkonfiguration von Kaspersky Endpoint Security**

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

   Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center installiert haben, wurde die Erstkonfiguration während der Installation automatisch gemäß den im Installationspaket angegebenen Parametern durchgeführt. Nach dem Abschluss der Installation müssen Sie die Anwendung auf ihren Einsatz vorbereiten.

   Wenn Sie Kaspersky Endpoint Security über die Befehlszeile installiert haben, starten Sie nach der Installation den Assistenten zur Erstkonfiguration und führen Sie die Erstkonfiguration der Anwendung im interaktiven Modus oder im automatischen Modus aus.

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

Light Agent-Modus

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

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

1. **Installation und Erstkonfiguration des Administrationsagenten**

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

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

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

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

   - Mit dem webbasierten Verwaltungs-Plug-in für Kaspersky Endpoint Security lässt sich 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.

   - Mit dem MMC-Verwaltungs-Plug-in von Kaspersky Endpoint Security können Sie das Programm über die Kaspersky Security Center Verwaltungskonsole verwalten. Das MMC-Plug-in muss auf dem Gerät installiert werden, auf dem die Kaspersky Security Center Verwaltungskonsole installiert ist.

3. **Installation von Anwendungspaketen und Erstkonfiguration von Kaspersky Endpoint Security**

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

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

Sie können die App auf eine der folgenden Arten installieren:

- Über Kaspersky Security Center.

  Vor der Installation müssen Sie die Parameter für die Erstkonfiguration der Anwendung entweder in den Parametern des Installationspakets oder in der Konfigurationsdatei angeben, die im Installationspaket enthalten ist.

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

  Der Parameterwert berücksichtigt Groß- und Kleinschreibung.

- Über die Befehlszeile. Wenn die Installation über die Befehlszeile durchgeführt wird, wird der Ausführungsmodus der Anwendung im Rahmen der Erstkonfiguration der Anwendung im interaktiven oder automatischen Modus ausgewählt.

4. **Erstkonfiguration von Kaspersky Endpoint Security**

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

Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center installiert haben, wurde die Erstkonfiguration während der Installation automatisch gemäß den im Installationspaket angegebenen Parametern durchgeführt. Nach dem Abschluss der Installation müssen Sie die Anwendung auf ihren Einsatz vorbereiten.

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

- Geben Sie im Schritt "Anwendung im Light Agent-Modus verwenden" des Assistenten zur Erstkonfiguration `yes` ein.
- Geben Sie in der Datei für die Erstkonfiguration den Parameter `KSVLA_MODE=Yes` an.

  Beim Wert der Einstellung muss die Groß- und Kleinschreibung beachtet werden.

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

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

Modus als Endpoint Detection and Response Agent

Es wird empfohlen, die Installation nach der Installation von Anti-Virus-Anwendungen von Drittanbietern auf dem Gerät auszuführen.

Wenn Sie Kaspersky Endpoint Security im Modus als Kaspersky Endpoint Security Agent verwenden möchten, umfasst die Installationsprozedur und Erstkonfiguration der Anwendung die folgenden Schritte:

1. **Installation und Erstkonfiguration des Administrationsagenten**

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

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

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

   - Mit dem webbasierten Verwaltungs-Plug-in für Kaspersky Endpoint Security lässt sich 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.

   - Mit dem MMC-Verwaltungs-Plug-in von Kaspersky Endpoint Security können Sie das Programm über die Kaspersky Security Center Verwaltungskonsole verwalten. Das MMC-Plug-in muss auf dem Gerät installiert werden, auf dem die Kaspersky Security Center Verwaltungskonsole installiert ist.

3. **Installation von Anwendungspaketen und Erstkonfiguration von Kaspersky Endpoint Security**

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

   Sie können die App auf eine der folgenden Arten installieren:

   - Über Kaspersky Security Center.

     Vor der Installation müssen Sie die Parameter für die Erstkonfiguration der Anwendung entweder in den Parametern des Installationspakets oder in der Konfigurationsdatei angeben, die im Installationspaket enthalten ist.

     Sie müssen den Modus als Endpoint Detection and Response Agent auswählen (Parameter `ENDPOINT_AGENT_MODE=Yes` in der Konfiogurationsdatei).

     Beim Wert der Einstellung muss die Groß- und Kleinschreibung beachtet werden.

   - Über die Befehlszeile. Wenn die Installation über die Befehlszeile durchgeführt wird, wird der Ausführungsmodus der Anwendung im Rahmen der Erstkonfiguration der Anwendung im interaktiven oder automatischen Modus ausgewählt.

4. **Erstkonfiguration von Kaspersky Endpoint Security**

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

Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center installiert haben, wurde die Erstkonfiguration während der Installation automatisch gemäß den im Installationspaket angegebenen Parametern durchgeführt. Nach dem Abschluss der Installation müssen Sie die Anwendung auf ihren Einsatz vorbereiten.

Wenn Sie Kaspersky Endpoint Security über die Befehlszeile installiert haben, starten Sie nach der Installation den Assistenten zur Erstkonfiguration und führen Sie die Erstkonfiguration der Anwendung im interaktiven Modus oder im automatischen Modus aus. Wählen Sie während der Erstkonfiguration den Modus als Endpoint Detection and Response Agent auf eine der folgenden Arten aus:

- Geben Sie im Schritt "Anwendung im Modus als Endpoint Detection and Response Agent verwenden" des Assistenten zur Erstkonfiguration `yes` ein.
- Geben Sie in der Datei für die Erstkonfiguration den Parameter `ENDPOINT_AGENT_MODE=Yes` an.

  Beim Wert der Einstellung muss die Groß- und Kleinschreibung beachtet werden.

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

Installation und Erstkonfiguration des Administrationsagenten von Kaspersky Security Center

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

Bevor mit der Installation des Administrationsagenten auf Geräten mit Linux-Betriebssystemen begonnen werden kann, müssen einige vorbereitende Schritte durchgeführt werden. Eine Beschreibung zur Vorbereitung von Geräten auf die Installation des Administrationsagenten finden Sie in der Hilfe zu Kaspersky Security Center. Der Umfang der erforderlichen Schritte hängt vom Betriebssystem ab.

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

- Per Fernzugriff vom Administrator-Arbeitsplatz aus über die Kaspersky Security Center Web Console oder über Verwaltungskonsole. Verwenden Sie für die Remote-Installation das Installationspaket des Administrationsagenten.
- Über die Befehlszeile:
  - Im Silent-Modus mit Antwortdatei. Eine Antwort-Datei ist eine Textdatei, die einen benutzerdefinierten Satz von Einstellungen für die Installation und Erstkonfiguration des Administrationsagenten enthält. Eine Beschreibung der Installationsparameter und der Ersteinrichtung des Administrationsagenten finden Sie in der Hilfe zu Kaspersky Security Center (im Abschnitt "Installation des Administrationsagenten für Linux im Silent-Modus (mit Antwortdatei)").
  - Im interaktiven Modus mittels RPM- oder DEB-Paket, je nach Art des verwendeten Paketmanagers. In diesem Fall müssen Sie nach der Installation die Erstkonfiguration des Administrationsagenten mithilfe eines Skripts durchführen.

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

Verwaltungs-Plug-ins für Kaspersky Endpoint Security installieren

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

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

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

Wenn Sie zur Verwaltung der Anwendung die Kaspersky Security Center Verwaltungskonsole verwenden, können Sie auch Richtlinien und Aufgaben, die mit früheren Versionen des Verwaltungs-Plug-ins erstellt wurden, in neue Versionen konvertieren.

Web-Plug-in für Kaspersky Endpoint Security installieren

Das Web-Plug-in für die Verwaltung von Kaspersky Endpoint Security muss auf dem Gerät installiert werden, auf dem auch 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.

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

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

  Sobald Sie die Kaspersky Security Center Web Console zum ersten Mal mit dem Administrationsserver verbinden, schlägt die Kaspersky Security Center Web Console automatisch vor, den Assistenten für die 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 Assistenten für die Ersteinrichtung der Kaspersky Security Center Web Console finden Sie in der Hilfe zu Kaspersky Security Center.

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

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

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

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

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

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

     a. Klicken Sie auf **Hinzufügen**.

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

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

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

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

     e. das Fenster **Konfiguration des Web-Plug-ins** wird geöffnet.

     > In Kaspersky Security Center Web Console Version 14.2 müssen Sie die Seite im Browser aktualisieren, damit das Fenster **"Konfiguration des Web-Plug-in**s" geöffnet wird.

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

   - Installation eines Web-Plug-ins aus einer Drittanbieter-Quelle (Archive, die zur Installation von Web-Plug-ins benötigt werden, sind im Lieferumfang enthalten und können von der Kaspersky-Website heruntergeladen werden):

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

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

     c. Klicken Sie auf **Hinzufügen**.

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

     e. das Fenster **Konfiguration des Web-Plug-ins** wird geöffnet.

     > In Kaspersky Security Center Web Console Version 14.2 müssen Sie die Seite im Browser aktualisieren, damit das Fenster **"Konfiguration des Web-Plug-in**s" geöffnet wird.

     f. 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.

MMC-Plug-in für Kaspersky Endpoint Security installieren

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

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:

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

Die Datei ist im Lieferumfang von Kaspersky Endpoint Security enthalten.

Nach der Installation wird das MMC-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:

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

2. Wählen Sie in der Liste links im Abschnitt **Erweitert** den Abschnitt **Informationen zu installierten 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**.

Installation und Erstkonfiguration der Anwendung mithilfe von Kaspersky Security Center

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

Die Installation mit Kaspersky Security Center besteht aus den folgenden Schritten:

1. Erstellen des Installationspakets.

Für die Remote-Installation wird ein Installationspaket für Kaspersky Endpoint Security verwendet. Das Installationspaket der Anwendung Kaspersky Endpoint Security ist für alle unterstützen Betriebssysteme und Architekturtypen des Prozessors gleich. Sie können ein Installationspaket über die Kaspersky Security Center Web Console oder über die Verwaltungskonsole erstellen.

Sie können die Parameter für die Erstkonfiguration der Anwendung entweder in den Einstellungen des Installationspakets oder in der Konfigurationsdatei "autoinstall.ini" angeben, die im Installationspaket enthalten ist.

Sie müssen die Einstellungen für die Erstkonfiguration der Anwendung konfigurieren, wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen (Teil der Lösung "Kaspersky Security for Virtualization Light Agent") oder im Modus als Endpoint Detection and Response Agent verwenden möchten. Standardmäßig wird die Anwendung im Standard-Modus verwendet.

Wenn Sie Kaspersky Endpoint Security im Standard-Modus oder im Modus als Endpoint Detection and Response Agent verwenden möchten, können Sie beim Erstellen des Installationspakets Folgendes zum Paket hinzufügen:

- Lizenzschlüssel zur automatischen Aktivierung der Anwendung während der Installation
- Vorab heruntergeladene Datenbanken für die Anwendung, um die Datenbanken nach der Installation nicht noch zusätzlich zu aktualisieren

Sie können die Anwendung auch später aktivieren und deren Datenbanken aktualisieren, wenn Sie die Anwendung auf ihre Ausführung vorbereiten.

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

2. Bereitstellung von Kaspersky Endpoint Security auf den Geräten im Netzwerk der Organisation.

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

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

   Die Kaspersky Security Center Verwaltungskonsole unterstützt die folgenden hauptsächlichen Bereitstellungsmethoden:

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

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

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

3. Vorbereiten der Anwendung auf ihre Ausführung.

   Vor der Verwendung der Anwendung muss die Erstkonfiguration der Anwendung abgeschlossen und die Anwendung auf ihre Ausführung vorbereitet werden.

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

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

Ein Installationspaket in der Web Console erstellen

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

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

Wenn Sie die Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen oder im Modus als Endpoint Detection and Response Agent verwenden möchten, müssen Sie in den Parametern der Erstkonfiguration den Nutzungsmodus der Anwendung angeben. Sie können die Parameter für die Erstkonfiguration der Anwendung wie folgt angeben: in den Eigenschaften des Installationspakets auf der Registerkarte **Einstellungen** oder in der Konfigurationsdatei, die im Installationspaket enthalten ist.

So bereiten Sie eine Archivdatei zum Erstellen eines Installationspakets vor:

1. Laden Sie das Archiv kesl.zip von der Download-Seite der App herunter. Es befindet sich unter **Kaspersky Endpoint Security für Linux** (**Zusätzliche Distribution** → **Dateien für die Remote-Installation des Produkts**).
2. Entpacken Sie das Archiv "kesl.zip" in einen Ordner, auf den der Administrationsserver von Kaspersky Security Center zugreifen kann. Legen Sie im selben Ordner die Dateien der Distribution ab, die dem Typ des Betriebssystems, in dem Sie die Anwendung installieren möchten, und dem Typ des Paketmanagers entsprechen:
   - für die Installation von Kaspersky Endpoint Security:
     - kesl-12.4.0-<Build-Nummer>.i386.rpm (für 32-Bit-Betriebssysteme mit rpm)
     - kesl_12.4.0-<Build-Nummer>_i386.deb (für 32-Bit-Betriebssysteme mit dpkg)
     - kesl-12.4.0-<Build-Nummer>.x86_64.rpm (für 64-Bit-Betriebssysteme mit rpm)
     - kesl_12.4.0-<Build-Nummer>_amd64.deb (für 64-Bit-Betriebssysteme mit dpkg)
     - kesl-12.4.0-<Build-Nummer>.aarch64.rpm (für 64-Bit-Betriebssysteme für Arm-Architektur mit rpm)
     - kesl_12.4.0-<Build-Nummer>_arm64.deb (für 64-Bit-Betriebssysteme für Arm-Architektur mit dpkg)

- für die Installation der grafischen Oberfläche der Anwendung:
  - kesl-gui-12.4.0-<Build-Nummer>.i386.rpm (für 32-Bit-Betriebssysteme mit rpm)
  - kesl-gui_12.4.0-<Build-Nummer>_i386.deb (für 32-Bit-Betriebssysteme mit dpkg)
  - kesl-gui-12.4.0-<Build-Nummer>.x86_64.rpm (für 64-Bit-Betriebssysteme mit rpm)
  - kesl-gui_12.4.0-<Build-Nummer>_amd64.deb (für 64-Bit-Betriebssysteme mit dpkg)
  - kesl-gui-12.4.0-<Build-Nummer>.aarch64.rpm (für 64-Bit-Betriebssysteme für Arm-Architektur mit rpm)
  - kesl-gui_12.4.0-<Build-Nummer>_arm64.deb (für 64-Bit-Betriebssysteme für Arm-Architektur mit dpkg)

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

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

Wenn Sie die grafische Oberfläche nicht installieren möchten, müssen Sie deren Verwendung deaktivieren, indem Sie den entsprechenden Parameter in den Eigenschaften des erstellten Installationspakets oder in der Konfigurationsdatei autoinstall.ini (`USE_GUI=No`) festlegen. Andernfalls wird die Installation mit einem Fehler beendet.

Wenn Sie das erstellende Installationspaket für verschiedene Betriebssysteme oder Paketmanagern verwenden möchten, platzieren Sie in diesem Ordner die Dateien für alle erforderlichen Betriebssysteme und Paketmanager.

3. Wenn Sie Kaspersky Endpoint Security im Standard-Modus mit bereits im Voraus heruntergeladene Datenbanken verwenden möchten:

   a. Platzieren Sie im Ordner die vorbereiteten Archive mit den Datenbanken für alle erforderlichen Betriebssysteme.

   b. Deaktivieren Sie in den Einstellungen zur Erstkonfiguration der Anwendung den Start der Aufgabe zum Datenbankupdate nach der Anwendungsinstallation. Sie können den entsprechenden Parameter in den Eigenschaften des erstellten Installationspakets oder in der Konfigurationsdatei autoinstall.ini (`UPDATE_EXECUTE=No`) konfigurieren. Die Datei "autoinstall.ini" befindet sich in dem Ordner, in den Sie das Archiv "kesl.zip" extrahiert haben.

4. Wenn Sie die Einstellungen für die Erstkonfiguration der Anwendung mithilfe einer Konfigurationsdatei konfigurieren möchten, öffnen Sie die Konfigurationsdatei autoinstall.ini und geben Sie die erforderlichen Änderungen ein.

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

Wenn Sie Kaspersky Endpoint Security im Modus als Endpoint Detection and Response Agent verwenden möchten, müssen Sie in der Konfigurationsdatei "autoinstall.ini" den Parameter `ENDPOINT_AGENT_MODE=Yes` festlegen.

Die Parameterwerte der Datei "autoinstall.ini" berücksichtigen die Groß- und Kleinschreibung.

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

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

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

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

   - **Entdeckung und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete**.
   - **Vorgänge → Datenverwaltung → Installationspakete**.

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

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Pakete wird gestartet.

3. Wählen Sie eine Methode zum Erstellen des Installationspakets:

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

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

4. Je nach gewählter Methode zum Erstellen eines Pakets:

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

5. 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. Mithilfe des Installationspakets können Sie die Anwendung auf Geräten im Unternehmensnetzwerk installieren oder die Version der Anwendung aktualisieren.

7. Konfigurieren Sie bei Bedarf die Parameter zur Erstkonfiguration der Anwendung. Öffnen Sie dazu die Eigenschaften des Installationspakets und wechseln Sie auf die Registerkarte **Parameter**.

   Kaspersky Security Center Web Console unterstützt erst ab Version 14.2 die Konfiguration der Parameter zur Erstkonfiguration in den Eigenschaften des Installationspakets von Kaspersky Endpoint Security. Verwenden Sie die Konfigurationsdatei autoinstall.ini, um die Einstellungen zu konfigurieren.

Parameter für die Erstkonfiguration in der Web Console

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**.

Sie können die Einstellungen für die Erstkonfiguration auch in der Konfigurationsdatei angeben, die im Installationspaket enthalten ist.

Parameter für die Erstkonfiguration der Anwendung

Parameter	Description
Sprache für Ereignisse in KSC	Wählen Sie die Sprache aus, die für die Lokalisierung der Anwendungsereignisse verwendet wird, die an Kaspersky Security Center gesendet werden: • **System** (Standardwert) – die 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 Landessprachen, die von Kaspersky Endpoint Security unterstützt werden. Die Anwendung verwendet die UTF-8-Kodierung. 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.
Anwendung aktivieren	Aktivieren Sie das Kontrollkästchen, wenn Sie die Anwendung während der Installation aktivieren möchten. Geben Sie im neuen Feld den Aktivierungscode ein. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Sie können die Anwendung auch nach der Installation aktivieren. Die Einstellung wird nur angewendet, wenn die Anwendung im Standard-Modus verwendet wird.

Parameter	Description
Update-Quelle	Wählen Sie die Update-Quelle 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. Der Parameter wird nur angewendet, wenn die Anwendung im Standard-Modus oder Modus als Endpoint Detection and Response Agent ausgeführt 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. Der Parameter wird nur angewendet, wenn die Anwendung im Standard-Modus oder Modus als Endpoint Detection and Response Agent ausgeführt wird.
Proxyserver-Einstellungen festlegen	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: • `[<Verbindungsprotokoll>://]<IP-Adresse des Proxyservers>:<Port>`, wenn für die Verbindung mit dem Proxyserver keine Authentifizierung erforderlich ist; • `[<Verbindungsprotokoll>://][<Benutzername>:[<Kennwort>]@]<IP-Adresse des Proxyservers>:<Port>`, wenn beim Verbinden mit dem Proxyserver eine Authentifizierung erforderlich ist. Das Herstellen einer Verbindung mit dem Proxyserver über das HTTPS-Protokoll wird nicht unterstützt. Der Parameter wird nur angewendet, wenn die Anwendung im Standard-Modus oder Modus als Endpoint Detection and Response Agent ausgeführt wird.
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.
Grafische Benutzeroberfläche verwenden	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die grafische Oberfläche der Anwendung installieren und verwenden möchten. Die Dateien zur Installation der grafischen Oberfläche müssen dafür dem Installationspaket hinzugefügt werden. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Der Parameter wird nur angewendet, wenn die Anwendung im Standard-Modus oder Modus als Endpoint Detection and Response Agent ausgeführt wird.
Benutzer die Administrator-Rolle (admin) zuweisen	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.
Auto-Konfiguration von SELinux ausführen	Bei aktiviertem Kontrollkästchen wird die automatische Konfiguration von SELinux für die Arbeit mit Kaspersky Endpoint Security ausgeführt. 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.

Parameter	Description
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.
Nutzungsmodus der Anwendung	Wählen Sie den Ausführungsmodus der Anwendung. • **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 zum Schutz virtueller Umgebungen verwendet (als Teil von Kaspersky Security for Virtualization Light Agent).
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.
Geschützte virtuelle Maschine als Server verwenden	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.
Abfangmechanismus	Wählen Sie den Mechanismus zum Abfangen von Systemereignissen, den die Anwendung im Rahmen ihrer Ausführung verwendet. • **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.

Parameter	Description
Wenn aktualisierbares Kernel-Modul nicht ausführbar	Wählen Sie die Aktion, die von der Anwendung ausgeführt wird, wenn das aktualisierbare Kernel-Modul aufgrund eines Fehlers 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.

Ein Installationspaket in der Administrationskonsole erstellen

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

Wenn Sie die Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen oder im Modus als Endpoint Detection and Response Agent verwenden möchten, müssen Sie in den Parametern der Erstkonfiguration den Nutzungsmodus der Anwendung angeben. Sie können die Parameter der Erstkonfiguration der Anwendung wie folgt angeben: bei der Erstellung des Installationspakets, nach der Erstellung in den Eigenschaften des Installationspakets im Abschnitt **Einstellungen** oder in der Konfigurationsdatei, die im Installationspaket enthalten ist.

So bereiten Sie Dateien für die Erstellung eines Installationspakets vor:

1. Laden Sie das Archiv kesl.zip von der Download-Seite der App herunter. Es befindet sich unter **Kaspersky Endpoint Security für Linux** (**Zusätzliche Distribution → Dateien für die Remote-Installation des Produkts**).

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

   - für die Installation von Kaspersky Endpoint Security:
     - kesl-12.4.0-<Build-Nummer>.i386.rpm (für 32-Bit-Betriebssysteme mit rpm)
     - kesl_12.4.0-<Build-Nummer>_i386.deb (für 32-Bit-Betriebssysteme mit dpkg)
     - kesl-12.4.0-<Build-Nummer>.x86_64.rpm (für 64-Bit-Betriebssysteme mit rpm)
     - kesl_12.4.0-<Build-Nummer>_amd64.deb (für 64-Bit-Betriebssysteme mit dpkg)
     - kesl-12.4.0-<Build-Nummer>.aarch64.rpm (für 64-Bit-Betriebssysteme für Arm-Architektur mit rpm)
     - kesl_12.4.0-<Build-Nummer>_arm64.deb (für 64-Bit-Betriebssysteme für Arm-Architektur mit dpkg)

- für die Installation der grafischen Oberfläche der Anwendung:
  - kesl-gui-12.4.0-<Build-Nummer>.i386.rpm (für 32-Bit-Betriebssysteme mit rpm)
  - kesl-gui_12.4.0-<Build-Nummer>_i386.deb (für 32-Bit-Betriebssysteme mit dpkg)
  - kesl-gui-12.4.0-<Build-Nummer>.x86_64.rpm (für 64-Bit-Betriebssysteme mit rpm)
  - kesl-gui_12.4.0-<Build-Nummer>_amd64.deb (für 64-Bit-Betriebssysteme mit dpkg)
  - kesl-gui-12.4.0-<Build-Nummer>.aarch64.rpm (für 64-Bit-Betriebssysteme für Arm-Architektur mit rpm)
  - kesl-gui_12.4.0-<Build-Nummer>_arm64.deb (für 64-Bit-Betriebssysteme für Arm-Architektur mit dpkg)

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

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

Wenn Sie die grafische Oberfläche nicht installieren möchten, müssen Sie deren Verwendung deaktivieren, indem Sie bei der Erstellung des Installationspakets den entsprechenden Parameter in den Eigenschaften des erstellten Installationspakets oder in der Konfigurationsdatei autoinstall.ini (`USE_GUI=No`) festlegen. Andernfalls wird die Installation mit einem Fehler beendet.

Wenn Sie das erstellende Installationspaket für verschiedene Betriebssysteme oder Paketmanagern verwenden möchten, platzieren Sie in diesem Ordner die Dateien für alle erforderlichen Betriebssysteme und Paketmanager.

3. Wenn Sie Kaspersky Endpoint Security im Standard-Modus mit bereits im Voraus heruntergeladene Datenbanken verwenden möchten:
   a. Platzieren Sie im Ordner die vorbereiteten Archive mit den Datenbanken für alle erforderlichen Betriebssysteme.
   b. Deaktivieren Sie in den Einstellungen zur Erstkonfiguration der Anwendung den Start der Aufgabe zum Datenbankupdate nach der Anwendungsinstallation. Sie können die entsprechende Einstellung beim Erstellen des Installationspakets, in den Eigenschaften des erstellten Installationspakets oder in der Konfigurationsdatei autoinstall.ini (`UPDATE_EXECUTE=No`) bearbeiten. Die Datei autoinstall.ini befindet sich in dem Verzeichnis, in das Sie das Archiv kesl.zip extrahiert haben.
4. Wenn Sie die Einstellungen für die Erstkonfiguration der Anwendung mithilfe einer Konfigurationsdatei konfigurieren möchten, öffnen Sie die Konfigurationsdatei autoinstall.ini und geben Sie die erforderlichen Änderungen ein.

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

Wenn Sie Kaspersky Endpoint Security im Modus als Endpoint Detection and Response Agent verwenden möchten, müssen Sie in der Konfigurationsdatei "autoinstall.ini" den Parameter `ENDPOINT_AGENT_MODE=Yes` festlegen.

Die Parameterwerte der Datei "autoinstall.ini" berücksichtigen die Groß- und Kleinschreibung.

Sie können die Parameter der Erstkonfiguration der Anwendung auch später konfigurieren, wenn Sie das Installationspaket erstellen oder im Abschnitt **Einstellungen** des erstellten Installationspakets.

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

1. Wählen Sie in der Konsolenstruktur den Punkt **Erweitert** → **Remote-Installation** → **Installationspakete** aus.
2. Klicken Sie auf **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. Müssen Sie ein Programmpaket von Kaspersky Endpoint Security auswählen. Öffnen Sie dazu mit der Schaltfläche **Durchsuchen** ein Windows-Standardfenster und geben Sie den Pfad zur Datei "kesl.kud" an. Die Datei befindet sich in dem Ordner, in den Sie das Archiv "kesl.zip" extrahiert haben.

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

   Wechseln Sie zum nächsten Schritt des Assistenten.
7. Konfigurieren Sie bei Bedarf die Parameter zur Erstkonfiguration der Anwendung.

   Sie können die Einstellungen für die Erstkonfiguration der Anwendung auch später in den Eigenschaften des erstellten Installationspakets im Abschnitt **Einstellungen** konfigurieren.
8. Der Assistent lädt die Dateien, die für die Installation der Anwendung erforderlich sind, auf den Administrationsserver von Kaspersky Security Center herunter. Warten Sie, bis die Installation abgeschlossen ist.
9. Schließen Sie den Assistenten ab.

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

Parameter für die Erstkonfiguration in der Verwaltungskonsole

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.

Sie können die Einstellungen für die Erstkonfiguration auch in der Konfigurationsdatei angeben, die im Installationspaket enthalten ist.

Parameter für die Erstkonfiguration der Anwendung

Parameter	Description
Sprache für Ereignisse in KSC	Wählen Sie die Sprache aus, die für die Lokalisierung der Anwendungsereignisse verwendet wird, die an Kaspersky Security Center gesendet werden: • **System** (Standardwert) – die Lokalisierungssprache des Betriebssystems. Wenn die Anwendung die Sprache des Betriebssystems nicht erkennt oder dessen Lokalisierung nicht unterstützt, wird Englisch als Standardsprache verwendet. • Eine der Landessprachen. Die Anwendung verwendet die UTF-8-Kodierung. 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 die Anwendung während der Installation aktivieren möchten, geben Sie den Aktivierungscode ein. Sie können die Anwendung auch nach der Installation aktivieren. Die Einstellung wird nur angewendet, wenn die Anwendung im Standard-Modus verwendet wird.
Auswahl der Update-Quellen	Durch Anklicken der Schaltfläche **Konfigurieren** wird ein Fenster geöffnet, in dem Sie die Update-Quelle für die Datenbanken und Module der Anwendung auswählen können: • **Kaspersky-Update-Server** (Standardwert). • **Kaspersky Security Center**. • **Andere Quellen im lokalen oder globalen Netzwerk**. Wenn Sie diese Option auswählen, geben Sie die Adresse der Update-Quelle in das Feld **Adresse** ein. Der Parameter wird nur angewendet, wenn die Anwendung im Standard-Modus oder Modus als Endpoint Detection and Response Agent ausgeführt 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. Der Parameter wird nur angewendet, wenn die Anwendung im Standard-Modus oder Modus als Endpoint Detection and Response Agent ausgeführt wird.

Parameter	Description
Adresse des Proxyservers	Wenn Sie für den Internetzugang einen Proxyserver verwenden, geben Sie die Adresse des Proxyservers in einem der folgenden Formate ein: • `[<Verbindungsprotokoll>://]<IP-Adresse des Proxyservers>:<Port>`, wenn für die Verbindung mit dem Proxyserver keine Authentifizierung erforderlich ist; • `[<Verbindungsprotokoll>://][<Benutzername>:[<Kennwort>]@]<IP-Adresse des Proxyservers>:<Port>`, wenn beim Verbinden mit dem Proxyserver eine Authentifizierung erforderlich ist. Das Herstellen einer Verbindung mit dem Proxyserver über das HTTPS-Protokoll wird nicht unterstützt. Der Parameter wird nur angewendet, wenn die Anwendung im Standard-Modus oder Modus als Endpoint Detection and Response Agent ausgeführt wird.
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.
Grafische Benutzeroberfläche verwenden	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die grafische Oberfläche der Anwendung installieren und verwenden möchten. Die Dateien zur Installation der grafischen Oberfläche müssen dafür dem Installationspaket hinzugefügt werden. Dieses Kontrollkästchen ist standardmäßig deaktiviert. Der Parameter wird nur angewendet, wenn die Anwendung im Standard-Modus oder Modus als Endpoint Detection and Response Agent ausgeführt wird.
Benutzer mit Administrator-Rolle (admin)	Geben Sie den Namen des Benutzers ein, 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.
Auto-Konfiguration von SELinux ausführen	Bei aktiviertem Kontrollkästchen wird die automatische Konfiguration von SELinux für die Arbeit mit Kaspersky Endpoint Security ausgeführt. 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.

Parameter	Description
Nutzungsmodus der Anwendung	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**, die das Fenster **Nutzungsmodus der Anwendung** öffnet. In diesem Fenster können Sie den Nutzungsmodus der Anwendung 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 zum Schutz virtueller Umgebungen verwendet (als Teil von Kaspersky Security for Virtualization Light Agent).
Geschützte virtuelle Maschine als Server verwenden (Fenster **Ausführungsmodus der Anwendung**)	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.
Modus zum Schutz der VDI-Infrastruktur aktivieren (Fenster **Ausführungsmodus der Anwendung**)	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.
Abfangen von Systemereignissen.	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Einstellungen für das Abfangen von Systemereignissen** geöffnet. In diesem Fenster können Sie den Mechanismus zum Abfangen von Systemereignissen auswählen, den die Anwendung im Rahmen ihrer Ausführung anwendet: • **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.
Wenn aktualisierbares Kernel-Modul nicht ausführbar (Fenster **Abfangen von Systemereignissen**)	Wählen Sie die Aktion, die von der Anwendung ausgeführt wird, wenn das aktualisierbare Kernel-Modul aufgrund eines Fehlers 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.

Vorbereitung eines Archivs mit Anwendungsdatenbanken zur Erstellung eines Installationspakets mit integrierten Datenbanken

Zur Durchführung einer Remote-Installation können Sie ein Installationspaket erstellen, das Anwendungsdatenbanken enthält, die bereits im Voraus heruntergeladen wurden. Dies kann beispielsweise erforderlich sein, wenn Sie die Anwendung auf einem Gerät mit dem Betriebssystem Astra Linux Special Edition installieren. 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.

So erstellen Sie ein Archiv mit Datenbanken für die Anwendungsinstallation:

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

2. Aktualisieren Sie die Anwendungsdatenbank. 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 der Kaspersky Security Center Verwaltungskonsole oder der Kaspersky Security Center Web Console eine Aufgabe vom Typ *Update* ausführen.

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

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

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

Parameter der Konfigurationsdatei "autoinstall.ini"

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

Der Parameterwert berücksichtigt Groß- und Kleinschreibung.

Parameter	Description	Werte
KSVLA_MODE	Verwendung von Kaspersky Endpoint Security im Light Agent-Modus.	`Yes` – Kaspersky Endpoint Security wird im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet (im Rahmen von Kaspersky Security for Virtualization Light Agent). `No` (Standardwert) – Kaspersky Endpoint Security wird im Standard-Modus oder im Modus als Endpoint Detection and Response Agent verwendet (siehe auch Parameter "ENDPOINT_AGENT_MODE").
SERVER_MODE	Rolle der geschützten virtuellen Maschine (Server oder Workstation). Die Einstellung wird nur angewendet, wenn die Anwendung im Light Agent-Modus verwendet wird.	`Yes` (Standardwert) – Die geschützte virtuelle Maschine wird als Server verwendet. `No` – Die geschützte virtuelle Maschine wird als Workstation verwendet.
VDI_MODE	Aktivieren des Modus zum Schutz der VDI-Infrastruktur, um die Leistung der Anwendung auf temporären virtuellen Maschinen zu optimieren. Die Einstellung wird nur angewendet, wenn die Anwendung im Light Agent-Modus verwendet wird.	`Yes` – Modus zum Schutz der VDI-Infrastruktur aktivieren. Dies wird empfohlen, wenn Kaspersky Endpoint Security auf einer Vorlage für virtuelle Maschinen installiert ist, aus der temporäre virtuelle Maschinen erstellt werden. `No` (Standardwert) – Modus zum Schutz der VDI-Infrastruktur nicht aktivieren.
ENDPOINT_AGENT_MODE	Verwendung von Kaspersky Endpoint Security im Modus als Endpoint Detection and Response Agent.	`Yes` – Kaspersky Endpoint Security wird im Modus als Endpoint Detection and Response Agent verwendet, um auf geschützten Geräten die gemeinsame Verwendung der Detection and Response-Lösungen von Kaspersky und der Antivirenlösungen von Drittanbietern zu gewährleisten. `No` (Standardwert) – Kaspersky Endpoint Security wird im Standard-Modus oder im Light Agent-Modus verwendet (siehe auch Parameter "KSVLA_MODE").
EULA_AGREED	Erforderliche Einstellung. Annahme der Bedingungen des Endbenutzer-Lizenzvertrags.	`Yes` (Standardwert) – Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren. `No` – Bedingungen des Endbenutzer-Lizenzvertrags nicht akzeptieren. Die Installation der Anwendung wird abgebrochen.
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 Anwendung wird abgebrochen.

Parameter	Description	Werte
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.
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` – Die Benutzer nicht aus privilegierten Gruppen entfernen.
LOCALE	Optionale Einstellung. Sprachstandard, der für die Lokalisierung von Ereignissen in der Anwendung 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 • `fr_FR.UTF-8` – Französisch • `ja_JP.UTF-8` – Japanisch • `ru_RU.UTF-8` – Russisch • `zh_TW.UTF-8` – Chinesisch (traditionell) • `zh_CN.UTF-8` – Chinesisch (vereinfacht) Wird die Einstellung `LOCALE` nicht angegeben, so 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.
INSTALL_LICENSE	Aktivierungscode zum Hinzufügen eines Lizenzschlüssels zur Anwendung. Die Einstellung wird nur angewendet, wenn die Anwendung im Standard-Modus verwendet wird.	`<Aktivierungscode>` – Wenn die Anwendung während der Installation aktiviert werden muss. `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. Der Parameter wird nur angewendet, wenn die Anwendung im Standard-Modus oder Modus als Endpoint Detection and Response Agent ausgeführt wird.	`SCServer` – Administrationsserver von Kaspersky Security Center als Update-Quelle verwenden `KLServers` – die Kaspersky-Update-Server als Update-Quelle verwenden Dieser Wert wird standardmäßig verwendet. `< Adresse der Update-Quelle >`

Parameter	Description	Werte
PROXY_SERVER	Adresse des Proxyservers, der für die Internetverbindung verwendet wird Der Parameter wird nur angewendet, wenn die Anwendung im Standard-Modus oder Modus als Endpoint Detection and Response Agent ausgeführt wird.	Adresse des Proxyservers in einem der folgenden Formate: • `[<Verbindungsprotokoll>://]<IP-Adresse des Proxyservers>:<Port>`, wenn für die Verbindung mit dem Proxyserver keine Authentifizierung erforderlich ist; • `[<Verbindungsprotokoll>://][<Benutzername>:[<Kennwort>]@]<IP-Adresse des Proxyservers>:<Port>`, wenn beim Verbinden mit dem Proxyserver eine Authentifizierung erforderlich ist. 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 Der Parameter wird nur angewendet, wenn die Anwendung im Standard-Modus oder Modus als Endpoint Detection and Response Agent ausgeführt wird.	`Yes` (Standardwert) – Update-Aufgabe starten. `No` – Update-Aufgabe nicht starten.
KERNEL_SRCS_INSTALL	Automatischer Start des Kompilierens der Kernel-Module beim Start des Schutzes vor bedrohlichen Dateien für Betriebssysteme, welche die fanotify-Technologie nicht unterstützen.	`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. Der Parameter wird nur angewendet, wenn die Anwendung im Standard-Modus oder Modus als Endpoint Detection and Response Agent ausgeführt 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.
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.
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.	`UseFanotify` (Standardwert) – fanotify-Technologie zum Abfangen von Systemereignissen verwenden. `UseUpdatableKernelModule` – Aktualisierbares Kernel-Modul zum Abfangen von Systemereignissen verwenden.
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.	`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. Der Parameter wird nur auf Geräten angewendet, deren Betriebssystem die fanotify-Technologie unterstützt.	`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` – Erstellt keine Protokolldatei beim ersten Start der Anwendung.

Wenn Sie die Einstellungen in der Konfigurationsdatei autoinstall.ini ändern möchten, geben Sie die Werte der Einstellungen im folgenden Format an: <Einstellungsname>=<Einstellungswert> ohne Leerzeichen zwischen dem

Namen der Einstellung und ihrem Wert.

Anwendung für die gemeinsame Ausführung mit Kaspersky Security Center vorbereiten

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

Standard-Modus

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

1. Aktivieren Sie die Anwendung, wenn die Aktivierung nicht mit dem Schlüssel aktiviert wurde, der den Installationspaket der Anwendung hinzugefügten wurde.

   Sie können die Aktivierungsaufgabe über die Verwaltungskonsole oder über die Kaspersky Security Center Web Console erstellen und ausführen. Alternativ dazu können Sie auch den Lizenzschlüssel aus dem Schlüsselspeicher von Kaspersky Security Center an die Geräte verteilen.

2. Aktualisieren Sie Datenbanken und Module der Anwendung, wenn dem Installationspaket der Anwendung keine Anwendungsdatenbanken hinzugefügt wurden, die bereits im Voraus heruntergeladen wurden. Sie können die *Update-Aufgabe* verwenden, die automatisch vom Assistenten bei der Erstkonfiguration von Kaspersky Security Center nach der Installation des MMC-basierten oder des webbasierten Verwaltungs-Plug-ins von Kaspersky Endpoint Security erstellt wird.

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

3. Konfigurieren Sie eine Richtlinie für die zentrale Verwaltung der App mithilfe der Kaspersky Security Center Verwaltungskonsole (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) oder der Web Console. Sie können die Richtlinie verwenden, die automatisch vom Assistenten bei der Erstkonfiguration von Kaspersky Security Center nach der Installation des MMC-Plug-ins oder des Web-Plug-ins für die Verwaltung von Kaspersky Endpoint Security erstellt wird.

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

Light Agent-Modus

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

1. Konfigurieren Sie Einstellungen der SVM-Erkennung durch die Light Agents. Dies benötigt die Erstellung und Konfiguration einer Richtlinie für die zentralisierte Verwaltung der Anwendungsausführung auf den Client-Geräten. Um Richtlinien zu verwalten, können Sie die Verwaltungskonsole (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) oder die Web Console verwenden.

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

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

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

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

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

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

   Nach der Aktivierung der Lösung auf den SVMs und der Verbindung der Light Agents mit den SVMs übermittelt der Schutzserver die Lizenzinformationen an die Light Agents. Sie können Informationen über die Lizenz, die von Kaspersky Endpoint Security als Teil der Lösung verwendet wird, entweder remote über Kaspersky Security Center oder direkt auf einer geschützten virtuellen Maschine über die Befehlszeile anzeigen.

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

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

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

Sie können Anwendungseinstellungen auch mithilfe der Richtlinien und Aufgaben zur Anwendungsverwaltung in der Verwaltungskonsole oder der Web Console konfigurieren.

Installation und Erstkonfiguration der Anwendung über die Befehlszeile

Sie können die Kaspersky Endpoint Security über die Befehlszeile auf einem Client-Gerät installieren.

Die Installation über die Befehlszeile besteht aus den folgenden Schritten:

1. Installation der Anwendung und der grafischen Oberfläche der Anwendung. Abhängig vom Modus, in dem Sie Kaspersky Endpoint Security verwenden möchten, können Sie die folgenden Installationsoptionen für die Anwendung verwenden:

   - Wenn Sie Kaspersky Endpoint Security im Standardmodus verwenden möchten, können Sie:
     - die Anwendung mit grafischer Oberfläche installieren
     - die Anwendung ohne grafische Oberfläche installieren
     - die grafische Oberfläche auf dem Gerät installieren, auf dem die Anwendung installiert ist

       Es ist nicht möglich, die grafische Oberfläche auf einem Gerät zu installieren, auf dem die Anwendung nicht installiert ist.

   - Wenn Sie die Kaspersky Endpoint Security im Light Agent-Modus verwenden möchten, müssen Sie die Anwendung ohne grafische Oberfläche installieren. Die grafische Oberfläche wird in diesem Modus nicht unterstützt.

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

2. Erstkonfiguration der Anwendung

   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 Erstkonfiguration der Anwendung erfolgt durch die Ausführung des Assistenten zur Erstkonfiguration, der im Lieferumfang von Kaspersky Endpoint Security enthalten ist. Sie können die Erstkonfiguration der Anwendung sowohl im interaktiven Modus als auch im automatisch Modus durchführen.

Anwendung über die Befehlszeile installieren

Installation der Anwendung ohne grafische Oberfläche der Anwendung

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

```
# rpm -i kesl-12.4.0-<Build-nummer>.i386.rpm
```

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

```
# rpm -i kesl-12.4.0-<Build-Nummer>.x86_64.rpm
```

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

```
# apt-get install kesl-12.4.0-<Build-Nummer>.x86_64.rpm
```

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

```
# rpm -i kesl-12.4.0-<Build-nummer>.aarch64.rpm
```

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

```
# apt-get install kesl-12.4.0-<Build-Nummer>.aarch64.rpm
```

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

```
# apt-get install ./kesl_12.4.0-<Build-Nummer>_i386.deb
```

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

```
# apt-get install ./kesl_12.4.0-<Build-Nummer>_amd64.deb
```

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

```
# apt-get install ./kesl_12.4.0-<Build-Nummer>_arm64.deb
```

Installation der grafischen Benutzeroberfläche der Anwendung

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

```
# rpm -i kesl-gui-12.4.0-<Build-Nummer>.i386.rpm
```

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

```
# rpm -i kesl-gui-12.4.0-<Build-Nummer>.x86_64.rpm
```

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

```
# apt-get install kesl-gui-12.4.0-<Build-Nummer>.x86_64.rpm
```

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

```
# rpm -i kesl-gui-12.4.0-<Build-Nummer>.aarch64.rpm
```

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

```
# apt-get install kesl-gui-12.4.0-<Build-Nummer>.aarch64.rpm
```

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

```
# apt-get install ./kesl-gui_12.4.0-<Build-Nummer>_i386.deb
```

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

```
# apt-get install ./kesl-gui_12.4.0-<Build-Nummer>_amd64.deb
```

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

```
# apt-get install ./kesl-gui_12.4.0-<Build-Nummer>_arm64.deb
```

Erstkonfiguration der Anwendung im interaktiven Modus

Um die Erstkonfiguration der Anwendung im interaktiven Modus durchzuführen, müssen Sie den Assistenten zur Erstkonfiguration von Kaspersky Endpoint Security ausführen.

Der Assistent zur Erstkonfiguration muss mit Root-Rechten ausgeführt werden.

Um den Assistenten zur Erstkonfiguration zu starten, führen Sie den folgenden Befehl aus:

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

Der Assistent fordert die Einstellungswerte für die Anwendung Kaspersky Endpoint Security schrittweise an. Sobald der Assistent abgeschlossen ist und die Befehlszeile freigegeben wird, ist der Prozess der Erstkonfiguration der Anwendung beendet.

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

```
echo $?
```

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

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

Anwendungsmodus auswählen: Standard oder Light Agent

In diesem Schritt planen Sie, ob Sie Kaspersky Endpoint Security im Light Agent-Modus verwenden möchten, um es als Kaspersky Security for Virtualization Light Agent zum Schutz virtueller Umgebungen einzusetzen.

- Geben Sie `yes` ein, wenn Sie Kaspersky Endpoint Security im Light Agent-Modus verwenden möchten.
- Geben Sie `no` ein, wenn Sie Kaspersky Endpoint Security im Standard-Modus verwenden möchten, um es als autonome Anwendung zum Schutz von Workstations und Servern einzusetzen.

  Wenn Sie vorhaben, die Anwendung im Modus als Endpoint Detection and Response Agent zu verwenden, müssen Sie in diesem Schritt `no` eingeben. Sie können den Modus als Endpoint Detection and Response Agent im nächsten Schritt auswählen.

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

Rolle der virtuellen Maschine festlegen

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

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

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

Die Rolle der virtuellen Maschine legt fest, unter welcher Lizenz die Anwendung auf dieser virtuellen Maschine verwendet wird und wie groß der verfügbare Funktionsumfang ist.

Modus zum Schutz der VDI-Infrastruktur aktivieren

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

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

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

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

Verwendungsmodus auswählen: Standard oder Endpoint Detection and Response Agent

Dieser Schritt wird nur angezeigt, wenn Sie im ersten Schritt als Nutzungsmodus für Kaspersky Endpoint Security den Standard-Modus ausgewählt haben. Die Anwendung kann nicht gleichzeitig im Light Agent-Modus und im Modus als Endpoint Detection and Response Agent verwendet werden.

In diesem Schritt geben Sie an, ob Sie vorhaben, die Anwendung "Kaspersky Endpoint Security" im Modus als Endpoint Detection and Response Agent zu verwenden:

- Geben Sie `yes` ein, wenn Sie Kaspersky Endpoint Security im Modus als Endpoint Detection and Response Agent verwenden möchten, damit die Anwendung auf geschützten Geräten die gemeinsame Verwendung der Detection and Response-Lösungen von Kaspersky und der Antivirenlösungen von Drittanbietern gewährleistet.
- Geben Sie `no` ein, wenn Sie Kaspersky Endpoint Security im Standard-Modus verwenden möchten, um es als autonome Anwendung zum Schutz von Workstations und Servern einzusetzen.

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

Sprachstandard auswählen

In diesem Schritt listet die Anwendung die unterstützten Sprachstandards im RFC 3066-Format auf.

Geben Sie den Sprachstandard in dem Format an, in dem er in der Liste angeführt 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.

Endbenutzer-Lizenzvertrag und Datenschutzrichtlinie lesen

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

Endbenutzer-Lizenzvertrag annehmen

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

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

- `yes` (oder `y`), wenn Sie 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.

Akzeptieren der Datenschutzrichtlinie

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

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

- `yes` (oder `y`), wenn Sie 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.

Verwendung von Kaspersky Security Network

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

Geben Sie einen der folgenden Werte ein:

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

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

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

Benutzer aus privilegierten Gruppen entfernen

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

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

Einem Benutzer die Administratorrolle zuweisen

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

Geben Sie den Namen des Benutzers ein, dem Sie die Administratorrolle zuweisen möchten. 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 auch später eine Administratorrolle zuweisen, nachdem Sie die Ersteinrichtung der Anwendung abgeschlossen haben.

Mechanismus zum Abfangen von Systemereignissen konfigurieren

In diesem Schritt wird die Möglichkeit festgelegt, verschiedene Mechanismen zum Abfangen von Systemereignissen in der Anwendung zu verwenden. Wenn das Betriebssystem auf dem Gerät die fanotify-Technologie unterstützt, können Sie den Mechanismus zum Abfangen von Systemereignissen auswählen, den die Anwendung im Rahmen ihrer Ausführung verwendet.

- 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.

Die Anwendung kann den auf dem aktualisierbaren Kernel-Modul basierenden Abfangmechanismus verwenden, wenn das Betriebssystem die Anforderungen an die Installation des Kernel-Moduls erfüllt. Wenn das Betriebssystem auf dem Gerät die fanotify-Technologie unterstützt, aber die Anforderungen an die Installation des aktualisierbaren Kernel-Moduls nicht erfüllt, verwendet die Anwendung die fanotify-Technologie, um Systemereignisse abzufangen.

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 `yes` 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.

Wenn das Betriebssystem auf dem Gerät die fanotify-Technologie nicht unterstützt, verwendet die Anwendung das Kernel-Modul zum Schutz vor bedrohlichen Dateien, um Systemereignisse abzufangen. Wenn alle notwendigen Pakete installiert wurden, wird das Kernel-Modul beim Start der Aufgabe zum Schutz vor bedrohlichen Dateien automatisch kompiliert.

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.

Automatische SELinux-Konfiguration aktivieren

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

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

Geben Sie `yes` ein, um die automatische Konfiguration des SELinux-Systems zu aktivieren. Wenn die automatische Konfiguration des SELinux-Systems fehlschlägt (z. B. weil das Tool semanage fehlt), gibt die Anwendung eine Fehlermeldung aus und fordert den Benutzer auf, das SELinux-System manuell zu konfigurieren.

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

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

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

Update-Quelle konfigurieren

Dieser Schritt wird nur angezeigt, wenn Sie bei den ersten Schritten des Assistenten die Verwendung von Kaspersky Endpoint Security im Standard-Modus oder im Modus als Endpoint Detection and Response Agent ausgewählt haben. Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, bezieht Kaspersky Endpoint Security die Updates für die Datenbanken und Anwendungsmodule von Light Agent über den Schutzserver.

In diesem Schritt müssen Sie die Quelle für die Updates der Datenbanken und Module der Anwendung angeben. 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 der benutzerdefinierten Update-Quelle im lokalen Netzwerk oder im Internet festlegen.

Allgemeine Proxy-Server-Einstellungen anpassen

Dieser Schritt wird nur angezeigt, wenn Sie bei den ersten Schritten des Assistenten die Verwendung von Kaspersky Endpoint Security im Standard-Modus oder im Modus als Endpoint Detection and Response Agent ausgewählt haben.

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

Führen Sie eine folgenden Aktionen aus, um die Einstellungen des Proxyservers anzupassen:

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

    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 für die Internetverbindung keinen Proxyserver verwenden, geben Sie `no` als Antwort ein.

Standardmäßig schlägt die Anwendung den Wert `no` vor.

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

Update der Anwendungsdatenbanken starten

Dieser Schritt wird nur angezeigt, wenn Sie bei den ersten Schritten des Assistenten die Verwendung von Kaspersky Endpoint Security im Standard-Modus oder im Modus als Endpoint Detection and Response Agent ausgewählt haben. Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, bezieht Kaspersky Endpoint Security die Updates für die Datenbanken und Anwendungsmodule von Light Agent über den Schutzserver.

In diesem Schritt können Sie die Aufgabe zum Update der Anwendungsdatenbanken auf dem Client-Gerät starten.

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

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

Standardmäßig wird von der Anwendung der Wert yes vorgeschlagen.

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

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.

Automatische Updates für die Anwendungsdatenbanken aktivieren

Dieser Schritt wird nur angezeigt, wenn Sie bei den ersten Schritten des Assistenten die Verwendung von Kaspersky Endpoint Security im Standard-Modus oder im Modus als Endpoint Detection and Response Agent ausgewählt haben. Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, bezieht Kaspersky Endpoint Security die Updates für die Datenbanken und Anwendungsmodule von Light Agent über den Schutzserver.

In diesem Schritt können Sie das automatische Anwendungsdatenbanken-Update aktivieren.

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.

Programm aktivieren

Dieser Schritt wird nur angezeigt, wenn Sie in den ersten Schritten des Assistenten als Nutzungsmodus für Kaspersky Endpoint Security den Standard-Modus ausgewählt haben. Wenn Kaspersky Endpoint Security im Modus als Endpoint Detection and Response Agent verwendet wird, müssen Sie nach der Ersteinrichtung der Anwendung den Lizenzschlüssel hinzufügen, der zur Aktivierung der Funktionalitäten von Kaspersky Endpoint Detection and Response Expert (on-premise) vorgesehen ist. Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, erhält Kaspersky Endpoint Security die Lizenzinformationen vom Schutzserver. Ein separates Aktivieren von Kaspersky Endpoint Security ist nicht erforderlich.

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

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

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

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.

Erstkonfiguration der Anwendung im automatischen Modus

Um die Erstkonfiguration der Anwendung im automatischen Modus durchzuführen, müssen Sie folgende Schritte durchführen:

1. Bereiten Sie eine Konfigurationsdatei vor, welche die Einstellungen für die Erstkonfiguration enthält. Sie können diese Datei erstellen oder ihre Struktur aus der Konfigurationsdatei "autoinstall.ini" kopieren, die zur Remote-Installation der Anwendung mithilfe von Kaspersky Security Center verwendet wird.

2. Führen Sie den Assistenten zur Erstkonfiguration von Kaspersky Endpoint Security aus und geben Sie dabei den Pfad zu der Konfigurationsdatei an.

   Der Assistent zur Erstkonfiguration muss mit Root-Rechten ausgeführt werden.

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

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

wobei `< Erstkonfigurationsdatei >` ein Pfad zur Konfigurationsdatei ist, die die Einstellungen der Erstkonfiguration enthält.

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

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

```
echo $?
```

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

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

Nach Abschluss des Assistenten müssen Sie für ein fehlerfreies Update der Anwendungsmodule die Anwendung neu starten. Überprüfen Sie den Update-Status der App mithilfe des Befehls `kesl-control --app-info`.

Einstellungen der Konfigurationsdatei für die Erstkonfiguration des Programms

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 Anwendung ab.

Der Parameterwert berücksichtigt Groß- und Kleinschreibung.

Einstellungen der Konfigurationsdatei für die Erstkonfiguration des Programms

Parameter	Description	Werte
KSVLA_MODE	Verwendung von Kaspersky Endpoint Security im Light Agent-Modus.	`Yes` – Kaspersky Endpoint Security wird im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet (im Rahmen von Kaspersky Security for Virtualization Light Agent). `No` – Kaspersky Endpoint Security wird im Standard-Modus oder im Modus als Endpoint Detection and Response Agent verwendet (siehe auch Parameter "ENDPOINT_AGENT_MODE").
SERVER_MODE	Rolle der geschützten virtuellen Maschine (Server oder Workstation). Die Einstellung wird nur angewendet, wenn die Anwendung im Light Agent-Modus verwendet wird.	`Yes` – Die geschützte virtuelle Maschine wird als Server verwendet. `No` – Die geschützte virtuelle Maschine wird als Workstation verwendet.
VDI_MODE	Aktivieren des Modus zum Schutz der VDI-Infrastruktur, um die Leistung der Anwendung auf temporären virtuellen Maschinen zu optimieren. Die Einstellung wird nur angewendet, wenn die Anwendung im Light Agent-Modus verwendet wird.	`Yes` – Modus zum Schutz der VDI-Infrastruktur aktivieren. Dies wird empfohlen, wenn Kaspersky Endpoint Security auf einer Vorlage für virtuelle Maschinen installiert ist, aus der temporäre virtuelle Maschinen erstellt werden. `No` – Modus zum Schutz der VDI-Infrastruktur nicht aktivieren.
ENDPOINT_AGENT_MODE	Verwendung von Kaspersky Endpoint Security im Modus als Endpoint Detection and Response Agent.	`Yes` – Kaspersky Endpoint Security wird im Modus als Endpoint Detection and Response Agent verwendet, um auf geschützten Geräten die gemeinsame Verwendung der Detection and Response-Lösungen von Kaspersky und der Antivirenlösungen von Drittanbietern zu gewährleisten. `No` – Kaspersky Endpoint Security wird im Standard-Modus oder im Light Agent-Modus verwendet (siehe auch Parameter "KSVLA_MODE").
EULA_AGREED	Erforderliche Einstellung. Annahme der Bedingungen des Endbenutzer-Lizenzvertrags.	`Yes` – Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren. `No` – Bedingungen des Endbenutzer-Lizenzvertrags nicht akzeptieren. Die Ersteinrichtung der Anwendung wird unterbrochen.
PRIVACY_POLICY_AGREED	Erforderliche Einstellung. Zustimmung zu den Bedingungen der Datenschutzrichtlinie.	`Yes`: Akzeptieren Sie die Datenschutzrichtlinie, um mit der Installation der App fortzufahren. `No` – Bedingungen der Datenschutzrichtlinie nicht akzeptieren. Die Ersteinrichtung der Anwendung wird unterbrochen.

Parameter	Description	Werte
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` – Bedingungen der Erklärung zu Kaspersky Security Network nicht akzeptieren. Das Ablehnen der Erklärung zu Kaspersky Security Network führt nicht zu einer Unterbrechung der Ersteinrichtung.
GROUP_CLEAN	Erforderliche Einstellung. 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` – Die Benutzer nicht aus privilegierten Gruppen entfernen.
LOCALE	Optionale Einstellung. Sprachstandard, der für die Lokalisierung von Ereignissen in der Anwendung 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 • `fr_FR.UTF-8` – Französisch • `ja_JP.UTF-8` – Japanisch • `ru_RU.UTF-8` – Russisch • `zh_TW.UTF-8` – Chinesisch (traditionell) • `zh_CN.UTF-8` – Chinesisch (vereinfacht) Wird die Einstellung `LOCALE` nicht angegeben, so 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.
INSTALL_LICENSE	Aktivierungscode oder Pfad zur Schlüsseldatei, um der Anwendung den Lizenzschlüssel hinzuzufügen. Die Einstellung wird nur angewendet, wenn die Anwendung im Standard-Modus verwendet wird.	`<Aktivierungscode>` – Wenn die Anwendung während der Installation mit einem Aktivierungscode aktiviert werden muss `<Vollständiger Pfad zur Schlüsseldatei>` – Wenn die Anwendung während der Installation mit einer Schlüsseldatei aktiviert werden muss `None` – Wenn die Anwendung während der Installation nicht aktiviert werden muss, etwa bei einer Installation in einem geschlossenen Netzwerksegment ohne Internetzugang.

Parameter	Description	Werte
UPDATER_SOURCE	Quelle für Updates der Datenbanken und Module der Anwendung aus. Der Parameter wird nur angewendet, wenn die Anwendung im Standard-Modus oder Modus als Endpoint Detection and Response Agent ausgeführt wird.	`SCServer` – Administrationsserver von Kaspersky Security Center als Update-Quelle verwenden `KLServers` – die Kaspersky-Update-Server als Update-Quelle verwenden `< Adresse der Update-Quelle >`
PROXY_SERVER	Adresse des Proxyservers, der für die Internetverbindung verwendet wird Der Parameter wird nur angewendet, wenn die Anwendung im Standard-Modus oder Modus als Endpoint Detection and Response Agent ausgeführt wird.	Adresse des Proxyservers in einem der folgenden Formate: • `[<Verbindungsprotokoll>://]<IP-Adresse des Proxyservers>:<Port>`, wenn für die Verbindung mit dem Proxyserver keine Authentifizierung erforderlich ist; • `[<Verbindungsprotokoll>://][<Benutzername>:[<Kennwort>]@]<IP-Adresse des Proxyservers>:<Port>`, wenn beim Verbinden mit dem Proxyserver eine Authentifizierung erforderlich ist. 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 Der Parameter wird nur angewendet, wenn die Anwendung im Standard-Modus oder Modus als Endpoint Detection and Response Agent ausgeführt wird.	`Yes` – Update-Aufgabe starten. `No` – Update-Aufgabe nicht starten.
KERNEL_SRCS_INSTALL	Automatischer Start des Kompilierens der Kernel-Module beim Start des Schutzes vor bedrohlichen Dateien für Betriebssysteme, welche die fanotify-Technologie nicht unterstützen.	`Yes` – Kernel-Modul beim Start des Schutzes vor bedrohlichen Dateien kompilieren. `No` – Kernel-Modul nicht kompilieren.
ADMIN_USER	Benutzer, dem die Administratorrolle (admin) zugewiesen ist.	
CONFIGURE_SELINUX	Automatische Konfiguration von SELinux für die Arbeit mit der Anwendung Kaspersky Endpoint Security.	`Yes` – Automatische Konfiguration von SELinux für die Arbeit mit Kaspersky Endpoint Security ausführen. `No` – keine automatische SELinux-Konfiguration durchführen.
DISABLE_PROTECTION	Deaktivieren der Schutzkomponenten und der Aufgaben Untersuchungsaufgaben der Anwendung, nachdem sie installiert wurde. Eine Installation mit deaktivierten Schutzkomponenten 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 und Aufgaben aktivieren, werden die aktivierten Komponenten und Aufgaben 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.

Parameter	Description	Werte
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.	`UseFanotify`, um die fanotify-Technologie zum Abfangen von Systemereignissen zu verwenden. `UseUpdatableKernelModule` – Aktualisierbares Kernel-Modul zum Abfangen von Systemereignissen verwenden.
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.	`FallbackToFanotify` – 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.
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` – Erstellt keine Protokolldatei beim ersten Start der Anwendung.

Geben Sie die Werte der Einstellungen im folgenden Format an: <Parametername>=<Parameterwert>, ohne Leerzeichen zwischen Name und Wert eines Parameters.

Zulassungsregeln im SELinux-System konfigurieren

Manuelle Konfiguration von SELinux für die Arbeit mit der Anwendung

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

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 wurde, führen Sie den folgenden Befehl aus:

     ```
     # setenforce Permissive
     ```

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

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

3. Wenn Sie eine benutzerdefinierte SELinux-Richtlinie verwenden, die sich von der Standardrichtlinie "targeted policy" unterscheidet, kennzeichnen Sie alle ausführbaren Quelldateien von Kaspersky Endpoint Security gemäß der verwendeten SELinux-Richtlinie mit folgendem Befehl:

   ```
   # semanage fcontext -a -t bin_t < ausführbare Datei >
   ```

   ```
   # restorecon -v < ausführbare Datei >
   ```

   Dabei steht `< ausführbare Datei >` für Folgendes:

   - /var/opt/kaspersky/kesl/12.4.0.<Build-Nummer>_<Installations-Zeitstempel>/opt/kaspersky/kesl/libexec/kesl
   - /var/opt/kaspersky/kesl/12.4.0.<Build-Nummer>_<Installations-Zeitstempel>/opt/kaspersky/kesl/bin/kesl-control
   - /var/opt/kaspersky/kesl/12.4.0.<Build-Nummer>_<Installations-Zeitstempel>/opt/kaspersky/kesl/libexec/kesl-gui
   - /var/opt/kaspersky/kesl/12.4.0.<Build-Nummer>_<Installations-Zeitstempel>/opt/kaspersky/kesl/shared/kesl

4. Führen Sie den folgenden Aufgaben aus:

   - Aufgabe zum Schutz vor bedrohlichen Dateien:

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

   - Aufgabe zur Untersuchung wichtiger Bereiche:

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

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

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

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

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

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

   ```
   # 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. Versetzen Sie das SELinux-System in den Sperrmodus:

   ```
   # 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.

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

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

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

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

     ```
     # setenforce Permissive
     ```

   - Falls SELinux deaktiviert wurde, geben Sie in der Konfigurationsdatei /etc/selinux/config den Parameterwert `SELINUX=permissive` an und starten Sie das Betriebssystem neu.
2. Stellen Sie sicher, dass das Tool semanage im System installiert ist. Wenn das Tool nicht installiert ist, installieren Sie je nach Typ des Paketmanagers das Paket policycoreutils-python oder policycoreutils-python-utils.
3. Führen Sie die Aufgabe "Prozess starten" aus.
4. Stellen Sie sicher, dass in der Datei "audit.log" keine Fehler enthalten sind:

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

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

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

6. Versetzen Sie das SELinux-System in den Sperrmodus:

   ```
   # setenforce Enforcing
   ```

Anwendung im Betriebssystem Astra Linux im Modus für abgeschlossene Softwareumgebungen starten

In diesem Abschnitt werden die Aktionen beschrieben, die Sie ausführen müssen, um die Anwendung unter Astra Linux Special Edition im Modus für geschlossene Softwareumgebungen zu starten.

Für Astra Linux Special Edition (reguläre Updates 1.6, 1.7 oder 1.8)

So starten Sie die Anwendung unter dem Betriebssystem Astra Linux Special Edition (reguläre Updates 1.6, 1.7 oder 1.8):

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

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Installieren Sie das Kompatibilitätspaket:

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

3. Erstellen Sie ein Verzeichnis für den Anwendungsschlüssel:

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

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

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

5. Aktualisieren Sie das initramfs-Image:

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

6. Starten Sie das Betriebssystem neu.

Für Astra Linux Special Edition (operational Update 1.5)

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

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

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

2. Erstellen Sie ein Verzeichnis für den Anwendungsschlüssel:

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

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

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

4. Aktualisieren Sie das initramfs-Image:

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

5. Starten Sie das Betriebssystem neu.

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

Anwendung im Betriebssystem ALT SP im Modus für geschlossene Softwareumgebungen starten

In diesem Abschnitt werden die Aktionen beschrieben, die Sie in der Befehlszeile ausführen müssen, um die Anwendung unter ALT SP im Modus für geschlossene Softwareumgebungen zu starten.

So starten Sie die Anwendung unter ALT SP:

1. Falls aktiviert, deaktivieren Sie den Modus für geschlossene Softwareumgebungen mit folgendem Befehl:

   ```
   integrity-remover
   ```

2. Erstellen Sie die Gruppe "kesl", um weitere Änderungen an der IMA-Richtlinie vorzunehmen, indem Sie folgenden Befehl ausführen:

   ```
   groupadd kesl
   ```

3. Ermitteln Sie die eindeutige Kennung (GUID) der erstellten Gruppe mit folgendem Befehl:

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

4. Bearbeiten Sie die IMA-Richtlinie, um die Gruppe "kesl" auszuschließen. Um dies zu tun:

   a. Kopieren Sie die Datei "/usr/share/integrity/policy" mit folgendem Befehl:

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

   b. Bearbeiten Sie die Datei "/etc/integrity/policy" mit einem Texteditor (z. B. vim), indem Sie folgenden Befehl ausführen:

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

   c. Fügen Sie nach der Zeile `dont_measure fsmagic=0xf97cff8c` (dies ist normalerweise die letzte Zeile im Abschnitt `dont_measure`) die Zeile `dont_measure fgroup=<GUID>` hinzu, wobei `<GUID>` die eindeutige ID der in Schritt 2 dieser Anleitung erstellten Gruppe ist).

   d. Fügen Sie nach der Zeile `dont_appraise fsmagic=0x27e0eb` (dies ist normalerweise die letzte Zeile im Abschnitt `dont_appraise`) die Zeile `dont_appraise fgroup=<GUID>` hinzu, wobei `<GUID>` die 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. Um dies zu tun:

   a. Bearbeiten Sie die Datei "usr/sbin/integrity-sign" mit einem Texteditor (z. B. vim), indem Sie folgenden Befehl ausführen:

      ```
      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.

6. Installieren Sie Kaspersky Endpoint Security. Um sicherzustellen, dass das Update der Datenbanken nach der Installation ordnungsgemäß funktioniert, lehnen Sie während der Ersteinrichtung der Anwendung den Start des Datenbanken-Updates ab (Geben Sie dazu im Schritt Start des Datenbanken-Updates der Anwendung "no" ein).

7. Weisen Sie den aktualisierten Komponenten von Kaspersky Endpoint Security die Vererbung der Gruppe "kesl" und der Verzeichnisberechtigungen zu, indem Sie die folgenden Befehle ausführen:

```
cd /var/opt/kaspersky/kesl/< Build-Nummer _*>/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 {} \;
```

8. Weisen Sie den aktualisierten Komponenten des Administrationsagenten die Vererbung der Gruppe "kesl" und der Verzeichnisberechtigungen zu, indem Sie die folgenden Befehle ausführen:

```
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 {} \;
```

9. Aktivieren Sie den Modus für geschlossen Softwareumgebungen durch Ausführen der Systemsignatur mit dem Befehl:

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

10. Stellen Sie sicher, dass das IMA-Subsystem aktiviert ist, indem Sie folgenden Befehl ausführen:

```
cat /proc/cmdline
```

Die Ausgabe des Befehls sollte diese Zeile enthalten: `lsm=integrity ima_hash=sha512 ima_appraise=enforce`.

11. Starten Sie die Aufgabe zum Datenbanken-Update mittels folgendem Befehl:

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

Wenn nach Abschluss des Datenbanken-Updates innerhalb der Ausgabe das Ereignis *EventType=BasesApplied* vorkommt, wurde das Datenbanken-Update erfolgreich abgeschlossen.

12. Starten Sie die Anwendung mittels folgendem Befehl neu:

```
systemctl restart kesl
```

Betriebssystem OSnova für die Ausführung der Anwendung konfigurieren

Für OSnova Version 2.4

So bereiten Sie ein Gerät mit dem Betriebssystem OSnova 2.4 auf die Remote-Installation des Administrationsagenten vor:

1. Öffnen Sie die Datei /etc/systemd/logind.conf und kommentieren Sie im Abschnitt `[Login]` die Zeile `#KillUserProcesses=yes` aus.

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

So starten Sie die Anwendung im Betriebssystem OSnova 2.4:

1. Öffnen Sie die Datei /etc/NESS/systemd/kesl.service.config und geben Sie den Parameterwert `NESSCTX_MODIFY=t+ADDEQUSOCK,OMIT,70,SSUID_SAVE_CTX_PERMANENT"` an.

2. Aktualisieren Sie die Einstellungen des Dienstes durch Ausführen des Befehls `systemctl daemon-reload`.

3. Wenn Sie die Überprüfung des Prozessspeichers und des Kernelspeichers durchführen möchten, müssen Sie den Speicherschutz mprotect (oder PaX) im Kernel deaktivieren. Fügen Sie dafür den Parameter `mprotect=off` zur Startbefehlszeile des Kernels hinzu. Weitere Informationen dazu finden Sie in der Dokumentaion zu OSnova.

4. Starten Sie das Betriebssystem neu.

Führen Sie nach der Installation der grafischen Benutzeroberfläche (Paket "kesl-gui") die folgenden Befehle im Terminal der Kommandozeile als Root aus:

```
rm /etc/xdg/autostart/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/autostart.desktop /etc/xdg/autostart/kaspersky-kesl.desktop

rm /usr/share/applications/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/app.desktop /usr/share/applications/kaspersky-kesl.desktop

rm /usr/share/autostart/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/autostart.desktop /usr/share/autostart/kaspersky-kesl.desktop

rm /usr/share/kde4/services/ServiceMenus/kaspersky-kesl.desktop
```

```
cp /opt/kaspersky/kesl/resource/kde.desktop
/usr/share/kde4/services/ServiceMenus/kaspersky-kesl.desktop

rm /usr/share/kservices5/ServiceMenus/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/kde.desktop /usr/share/kservices5/ServiceMenus/kaspersky-
kesl.desktop

rm /usr/share/Thunar/sendto/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/sendto.desktop /usr/share/Thunar/sendto/kaspersky-
kesl.desktop
```

Für OSnova Version 2.5.1 oder höher

So bereiten Sie ein Gerät mit dem Betriebssystem OSnova 2.5.1 oder höher auf die Remote-Installation des Administrationsagenten vor:

1. Öffnen Sie die Datei /usr/lib/systemd/logind.conf.d/10-enable-kill-user-processes.conf und kommentieren Sie im Abschnitt `[Login]` die Zeile `#KillUserProcesses=yes` aus.
2. Öffnen Sie die Datei /usr/lib/NESS/pam-user-session und kommentieren Sie die Zeile `#loginctl terminate-session "$XDG_SESSION_ID"` aus.

So starten Sie die Anwendung im Betriebssystem OSnova 2.5.1 und höher:

1. Öffnen Sie die Datei /etc/NESS/systemd/kesl.service.config und legen Sie den Parameter `NESSCTX_MODIFY="t+ADDEQUSOCK,OMIT,OMIT_PID,SSUID_SAVE_CTX_PERMANENT"` fest.
2. Aktualisieren Sie die Einstellungen des Dienstes durch Ausführen des Befehls `systemctl daemon-reload`.
3. Öffnen Sie die Datei /etc/sysctl.d/30-disable-ptrace.conf und setzen Sie `kernel.yama.ptrace_scope=0.`.
4. Wenn Sie die Überprüfung des Prozessspeichers und des Kernelspeichers durchführen möchten, müssen Sie den Speicherschutz mprotect (oder PaX) im Kernel deaktivieren. Fügen Sie dafür den Parameter `mprotect=off` zur Startbefehlszeile des Kernels hinzu. Weitere Informationen dazu finden Sie in der Dokumentaion zu OSnova.
5. Starten Sie das Betriebssystem neu.

Bei der Installation der Anwendung "Kaspersky Endpoint Security" auf einem Gerät mit OSnova Version 2.14 und höher kann aufgrund eines doppelten Vorhandenseins der Zeile `SUPPORT_URL` in der Datei "/etc/os-release" der folgende Fehler auftreten: `"dpkg: error processing package kesl (--install): installed kesl package post-installation script subprocess returned error exit status 1"`. Um die Anwendung ordnungsgemäß zu installieren, müssen Sie in der Datei "/etc/os-release" eine der beiden `SUPPORT_URL`-Zeilen löschen.

Optimierung der Ressourcenauslastung durch die Anwendung

Dieser Abschnitt enthält Empfehlungen von Kaspersky-Experten zur Konfiguration von Kaspersky Endpoint Security, um die Auslastung von Systemressourcen zu optimieren. 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. Um Leistungseinbußen zu vermeiden, wird es empfohlen, nach der Installation und Erstkonfiguration der Anwendung die in diesem Abschnitt beschriebenen Verfahren zu befolgen.

Das empfohlene Szenario zur Konfiguration der Anwendung für eine optimale Ausnutzung der Systemressourcen besteht aus folgenden Schritten:

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**

   Führen Sie die empfohlene Konfiguration der Anwendung auf den Geräten durch, die dieser Rolle in der Infrastruktur entsprechen.

3. **Durchführen einer Leistungsanalyse auf Mustergeräten**

   Wählen Sie in jeder Gruppe 1-2 Geräte aus, die als Mustergeräte dienen. 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.

   Sie können auch die Ausführung der Komponenten Schutz vor Web-Bedrohungen und Schutz vor Netzwerkbedrohungen optimieren.

5. **Konfiguration der Anwendungseinstellungen 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.

Empfehlungen für typische Serverrollen

Webserver

Bei Verwendung des HTTPS-Protokolls und bei hoher Client-Auslastung auf dem Server können die Komponenten Schutz vor Web-Bedrohungen und Schutz vor Netzwerkbedrohungen 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 Servers ändert, während diese Komponenten ausgeführt werden. Wenden Sie sich an den Technischen Support von Kaspersky, um die optimalen Ausführungsparameter auszuwählen und Kompatibilitätsprobleme zu lösen.

Proxy-Server

Es wird empfohlen, die Komponenten Schutz vor Web-Bedrohungen und Schutz vor Netzwerkbedrohungen auf dem Gerät zu deaktivieren, das als Proxyserver oder Load Balancer verwendet wird.

Server mit Containern

Es wird empfohlen, die Komponenten Schutz vor Web-Bedrohungen und Schutz vor Netzwerkbedrohungen auf den Servern zu deaktivieren, die als Container-Server verwendet werden. Für den Schutz von Container-Umgebungen kann die Anwendung Kaspersky Container Security verwendet werden.

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.

Um Informationen über den Ressourcenverbrauch der Anwendung anzuzeigen, führen Sie den folgenden Befehl aus:

```
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.

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 über die Kommandozeile folgende Tests auf dem Gerät durch:

1. Analysieren Sie den Ressourcenverbrauch der Aufgabe "Schutz vor bedrohlichen Dateien" (Aufgabentyp "OAS"). Dadurch können Sie feststellen, ob die Leistungsprobleme mit der Aufgabe "Schutz vor bedrohlichen Dateien" oder mit Untersuchungsaufgaben (Aufgabentypen "ODS" und "ContainerScan") zusammenhängen, und die Empfehlungen für die entsprechenden Aufgaben befolgen.

2. Identifizieren Sie die am häufigsten untersuchten Objekte. Die Leistung der Anwendung kann optimiert werden, indem ungefährliche Objekte und Dateien von der Untersuchung ausgeschlossen werden.

Die Analyse der Aufgabenausführung findet über die Befehlszeile statt. Wenn die Anwendung durch eine Richtlinie von Kaspersky Security Center verwaltet wird, muss für die Dauer der Überprüfung die Verwaltung lokaler Aufgaben zugelassen werden.

Nutzung der Ressourcen durch die Aufgabe zum Schutz vor bedrohlichen Dateien analysieren

So analysieren Sie die Nutzung von Ressourcen durch die 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 mit allen Aufgaben der Anwendung ab, indem Sie den folgenden Befehl ausführen:

   ```
   Befehl kesl-control --get-task-list
   ```

   b. Rufen Sie die Zeitplaneinstellungen für aller Audfgaben der Typen "ODS" und "ContainerScan" ab, indem Sie den folgenden Befehl ausführen:

   ```
   kesl-control --get-schedule <ID/Name der Aufgabe>
   ```

   Wenn der Befehl `RuleType=Manual` ausgibt, wird die Aufgabe nur manuell ausgeführt.

   c. Ändern Sie für alle Aufgaben, für die der Wert des Parameters `RuleType` nicht `Manual` beträgt, den Startzeitplan, indem Sie den folgenden Befehl ausführen:

   ```
   kesl-control --set-schedule <ID/Name der Aufgabe> RuleType=Manual
   ```

3. Aktivieren Sie die Erstellung von Protokolldateien mit hohem Detaillierungsgrad für die Anwendung, indem Sie den folgenden Befehl ausführen:

   ```
   kesl-control --set-app-settings TraceLevel=Detailed
   ```

4. Starten Sie die Aufgabe zum Schutz vor bedrohlichen Dateien (falls diese nicht bereits läuft) mit dem folgenden Befehl:

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

5. Sorgen Sie für eine Systemauslastung im gleichen Modus, der die Leistungsprobleme verursacht hat. Es genügen einige Stunden.

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.

   Sollten 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 der Anwendung, indem Sie den folgenden Befehl ausführen:

   ```
   kesl-control --set-app-settings TraceLevel=None
   ```

Am häufigsten untersuchte Objekte identifizieren

Sie erhalten eine Liste der Objekte, die am häufigsten untersucht wurden, indem Sie den folgenden Befehl ausführen:

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | sort | uniq -c |
sort -k1 -n -r|less
```

Das Ergebnis wird in der Anwendung zum Betrachten von Textdateien "less" angezeigt, wobei die Objekte, die am häufigsten untersucht wurden, ganz am Anfang stehen.

Wenn Sie in Verzeichnen Statistiken über untersuchte Objekt in bestimmten Verzeichnisebenen (ausgehend vom Stammverzeichnis `/`) aggregieren möchten, können Sie den Befehl mit `cut -d/ -f 1-X` erweitern. Dabei steht das "X" für die Tiefe der Verzeichnisebenen, z. B.:

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | cut -d/ -f 1-4 |
sort | uniq -c | sort -k1 -n -r|less
```

Wenn mehrere Dienste im System häufig in Dateien schreiben, werden solche Dateien wiederholt in einer verzögerten Warteschlange untersucht. Sie erhalten eine Liste der Pfade, die am häufigsten in einer verzögerten Warteschlange untersucht wurden, indem Sie den folgenden Befehl ausführen:

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk
'{print $10}' | sort | uniq -c | sort -k1 -n -r
```

Die Dateien, die am häufigsten untersucht wurden, werden am Anfang der Liste angezeigt.

Wenn Sie in Verzeichnen Statistiken über untersuchte Objekt in bestimmten Verzeichnisebenen (ausgehend vom Stammverzeichnis `/`) aggregieren möchten, können Sie den Befehl mit `cut -d/ -f 1-X` erweitern. Dabei steht das "X" für die Tiefe der Verzeichnisebenen, z. B.:

```
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
```

Es wird empfohlen, zu überprüfen, ob die am häufigsten untersuchten Objekte und Dateien gefährlich sind. Ungefährliche Objekte oder Dateien können den Ausnahmen hinzugefügt werden, um die Ausführung des Schutzes vor bedrohlichen Dateien und der Untersuchungsaufgaben zu optimieren. 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.

Empfehlungen für den Schutz vor bedrohlichen Dateien und die Untersuchungsaufgaben

Optimieren des Schutzes vor bedrohlichen Dateien

Um die Ausführung der Komponente "Schutz vor bedrohlichen Dateien" zu optimieren, können Sie Folgendes tun:

- Konfigurieren von Untersuchungsausnahmen für Objekte, die am häufigsten untersucht werden, aber ungefährlich sind.
- Konfigurieren von Ausnahmen für das Abfangen von Dateivorgängen.
- 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 mithilfe des folgenden Befehls:

    ```
    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.
- Sicherstellen, dass die Untersuchung von Archiven deaktiviert ist (Standardwert). 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.
- Festlegen einer Obergrenze des von der Anwendung genutzten Arbeitsspeichers.

Optimieren von Untersuchungsaufgaben

Um die Ausführung der Untersuchungsaufgaben (Aufgaben der Typen "ODS" und "ContainerScan") zu optimieren, können Sie Folgendes tun:

- 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.
- Ausführen der Untersuchung zum Zeitpunkt der geringsten Serverauslastung.
- Sicherstellen, dass sich im Untersuchungsbereich der Untersuchungsaufgaben keine Remote-Verzeichnisse befinden, die mittels SMB- und NFS-Protokoll auf dem Gerät gemountet 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).
- Konfigurieren von Untersuchungsausnahmen für Objekte, die am häufigsten untersucht werden, aber ungefährlich sind.
- Konfigurieren von Ausnahmen für das Abfangen von Dateivorgängen.
- Festlegen einer Obergrenze des von der Anwendung genutzten Arbeitsspeichers.

Untersuchungsausnahmen konfigurieren

Anhand von Untersuchungsausnahmen kann ein Mittelwert zwischen Schutz und Leistung des Systems erreicht werden. Laut den Virenexperten von Kaspersky können Daten- und Indexdateien von Datenbanken bedenkenlos zu den Ausnahmen hinzugefügt werden. Es wird angenommen, dass keine Gefahr besteht, dass Viren über solche Dateien eindringen.

Die ungefährlichen Objekte aus der Liste der am häufigsten untersuchten Dateien können von der Untersuchung ausgeschlossen werden.

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. Sollten sich selbst minimale Verzögerungen für die Ausführung des Systems als kritisch erweisen, wird es empfohlen, Ausnahmen für das Abfangen von Dateivorgängen zu konfigurieren.

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 auch Ausnahmen für Untersuchungsaufgaben vom Typ "ODS" und "ContainerScan" konfigurieren. Die Ausnahmen werden über die Aufgabeneinstellungen in Kaspersky Security Center oder über die lokale Befehlszeile auf dem Gerät festgelegt.

Die Einstellungen für die Untersuchungsausnahmen einer Untersuchungsaufgabe werden nicht an andere Untersuchungsaufgaben übertragen. Sie müssen für jede Aufgabe zur Untersuchung eigene Ausschlüsse konfigurieren.

Nachfolgend finden Sie Beispiele zur Konfiguration von Ausnahmen des Schutzes vor bedrohlichen Dateien über die Befehlszeile.

Um das Verzeichnis /tmp/logs und alle Unterverzeichnisse und Dateien rekursiv auszuschließen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

Um eine bestimmte Datei oder Dateien nach Maske im Verzeichnis /tmp/logs auszuschließen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

Um alle Dateien mit der Erweiterung .log im Verzeichnis /tmp/ und in den Unterverzeichnissen rekursiv anhand einer Maske auszuschließen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

Ausnahmen für das Abfangen von Dateivorgängen konfigurieren

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.

Mit dem folgenden Befehl können Sie Statistiken zu den von der Anwendung abgefangenen Dateien abrufen:

```
kesl-control --get-statistic --files
```

Der Befehl gibt die Statistiken zu den abgefangenen Dateivorgängen der letzten 24 Stunden aus.

Bei Bedarf können Sie mithilfe der Anwendungs-Protokolle eine detailliertere Analyse durchführen. Standardmäßig werden keine Protokolldateien erstellt. Sie können die Erstellung von Protokolldateien mit dem folgenden Befehl 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.

Die Erstellung von Protokolldateien kann mit dem folgenden Befehl deaktiviert werden:

```
kesl-control --set-app-settings TraceLevel=None
```

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. Die Liste mit den abgefangenen Dateien erhalten Sie durch das Ausführen des folgenden Befehls:

```
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 in Verzeichnen Statistiken über abgefangene Dateivorgänge in bestimmten Verzeichnisebenen (ausgehend vom Stammverzeichnis `/`) aggregieren möchten, können Sie den Befehl mit `cut -d/ -f 1-X` erweitern. Dabei steht das "X" für die Tiefe der Verzeichnisebenen, z. B.:

```
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
```

Um die Dateien eines bestimmten Verzeichnisses nicht nur von der Untersuchung, sondern auch vom Abfangen auszuschließen, müssen Sie den gesamten Mountpunkt ausschließen. Durch das Ausschließen von Mountpunkten (globale Ausnahme) können Sie lokale oder Remote-Verzeichnisse, die auf dem Gerät gemountet sind, vom Modul zum Abfangen von Dateioperationen ausschließen.

Für Pfade, die keine Mountpunkte darstellen, gelten keine globalen Ausnahmen.

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.

Um gemeinsam genutzte Netzwerkressourcen zu schützen, können Sie Kaspersky Endpoint Security direkt auf dem Gerät verwenden, welches die Ressourcen physisch speichert.

Sie können globale Ausnahmen innerhalb einer Richtlinie über die Web Console, die Verwaltungskonsole oder lokal auf dem Gerät anhand der Befehlszeile konfigurieren.

Nachfolgend ist ein Beispiel für die Konfiguration einer Ausnahme zum Abfangen von Dateivorgängen über die Befehlszeile aufgeführt.

So schließen Sie alle Dateien im Verzeichnis /tmp vom Abfangen aus:

1. Wenn das Verzeichnis kein Mountpunkt ist, müssen Sie einen Mountpunkt daraus erstellen. Um beispielsweise einen Mountpunkt aus dem Verzeichnis /tmp zu erstellen, führen Sie den folgenden Befehl aus:

   ```
   mount --bind /tmp/ /tmp
   ```

2. Tragen Sie in die Datei /etc/fstab die folgende Zeile ein, damit der Mountpunkt nach dem Neustart des Servers erhalten bleibt:

   ```
   /tmp /tmp none defaults,bind 0 0
   ```

3. Fügen Sie das Verzeichnis /tmp zu den globalen Ausschlüsse hinzu, indem Sie den folgenden Befehl ausführen:

   ```
   kesl-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
   ```

4. Wenn Sie mehrere Verzeichnisse hinzufügen möchten, erhöhen Sie den Zähler item_0000 jeweils um eine Einheit (item_0001, item_0002 usw.).

Begrenzung des Speicherverbrauchs der Anwendung festlegen

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 mittels des Parameters `ScanMemoryLimit=<Menge des Speichers in Megabyte>` 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.

Empfehlungen für den Schutz vor Web-Bedrohungen und den Schutz vor Netzwerkbedrohungen

Um die Auswirkungen der Komponenten Schutz vor Web-Bedrohungen und Schutz vor Netzwerkbedrohungen auf die Ausführung der Benutzeranwendungen zu reduzieren, wird es empfohlen, Folgendes zu tun:

- Betriebssystem-Firewall konfigurieren. Wenn das System über eigene oder (firwalld-) Netzwerkregeln mit Drop-Richtlinien verfügt, müssen Sie für eine ordnungsgemäße Ausführung der Anwendung eine Erlaubnisregel hinzufügen, um eingehende lokale Verbindungen des Geräts (loopback) zu erlauben.

  Beispielbefehl für iptables:

  ```
  iptables -A INPUT -i lo -j ACCEPT
  ```

- Kompatibilität der REDIRECT-Regel (z. B. Umleitung von Port 443 auf 8443) mit den Abfangregeln des Schutzes vor Netzwerkbedrohungen gewährleisten. Dafür müssen Sie:

  a. Die Regel löschen:

  ```
  iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
  ```

  b. Stattdessen die folgenden Regeln hinzufügen:

  ```
  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
  ```

- Richtlinie zur Überprüfung von Zertifikaten konfigurieren. 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 besitzt, müssen Sie eine lokale Methode (ohne Verwendung des Internets) zur Überprüfung der Zertifikate durch die Anwendung auswählen oder einen Proxyserver für den Internetzugang verwenden.

  Sie können in den Einstellungen der Untersuchung des Netzwerkverkehrs eine lokale Methode zur Überprüfung von Zertifikaten auswählen:

  - 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 mithilfe des folgenden Befehls:

    ```
    kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
    ```

  Die Anwendung überpüft Zertifikate ohne das Internet zu verwenden.

  Sie können die Verwendung eines Proxyservers aktivieren und dessen Einstellungen in einer Richtlinie mithilfe der Web Console, der Verwaltungskonsole oder lokal über die Befehlszeile konfigurieren.

- Die Liste der von der Anwendung kontrollierten Netzwerkports begrenzen. 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`.

Wenn Sie die Anwendung zusammen mit dem Balancer HAProxy verwenden, wird es empfohlen, die folgenden Maßnahmen auszuführen:

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 die Anwendung neu:

   ```
   systemctl restart kesl
   ```

Die gemeinsame Ausführung der Schutzkomponenten des Schutzes vor Web-Bedrohungen, des Schutzes vor Netzwerkbedrohungen und der Kubernetes-Containerisierung erfordert eine zusätzliche, fein abgestimmte und arbeitsintensive Konfiguration der Betriebssystem-Firewall. Die gemeinsame Ausführung von Kubernetes mit Cillium CNI ist nicht möglich.

Update einer Vorgängerversion der Anwendung durchführen

Ein Upgrade auf Kaspersky Endpoint Security 12.4 für Linux ist nur für die Version Kaspersky Endpoint Security 12.3 für Linux möglich.

Es ist nicht möglich, Kaspersky Endpoint Security von früheren Versionen auf Version 12.4 zu aktualisieren. Wenn Sie eine frühere Version von Kaspersky Endpoint Security installiert haben, müssen Sie diese zunächst deinstallieren und anschließend Kaspersky Endpoint Security 12.4 für Linux installieren.

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

Die Aktualisierung der Anwendung besteht aus den folgenden Schritten:

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

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

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

   Während des Updates des Administrationsagenten funktioniert die Anwendung weiterhin ordnungsgemäß.

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

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

3. **Aktualisieren der Anwendung und der grafischen Oberfläche auf geschützten Geräten**

   Sie müssen die auf den geschützten Geräten installierte Anwendung aktualisieren. 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 Standard-Modus oder im Modus als Endpoint Detection and Response Agent verwenden und die grafische Benutzeroberfläche der Anwendung nutzen, sollten Sie diese ebenfalls aktualisieren.

Sie können die Anwendung und die grafische Oberfläche der Anwendung auf folgende Weise aktualisieren:

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

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

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

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

Beim Aktualisieren der Anwendungsversion wird die Datei der Ereignisdatenbank der vorherigen Version im Dateisatz der aktuellen Version zur ersten Datei mit Ereignissen. 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 Standard-Modus oder im Modus als Endpoint Detection and Response Agent ausgeführt wird, wird es empfohlen, nach einer Anwendungsaktualisierung die Datenbanken zu aktualisieren.

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

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

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

Richtlinien und Aufgaben, die für 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 Anwendung konfiguriert wurden. Einige Parameter verfügen über spezielle Werte. Parameter, die in den Richtlinien und Aufgaben der vorherigen Version nicht enthalten waren, übernehmen in den konvertierten Richtlinien und Aufgaben die vorgesehenen Standardwerte.

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

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

Wenn Sie die 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.

Update der Anwendung mithilfe von Kaspersky Security Center durchführen

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

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

Das Update über Kaspersky Security Center besteht aus den folgenden Schritten:

1. Erstellen des Installationspakets.

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

2. Bereitstellung von Kaspersky Endpoint Security auf den Geräten im Netzwerk der Organisation.

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

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

   Die Kaspersky Security Center Verwaltungskonsole unterstützt die folgenden hauptsächlichen Bereitstellungsmethoden:

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

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

Update der Anwendung über die Befehlszeile durchführen

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

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

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

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

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

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. Lesen Sie die neue Version des Dokuments im Verzeichnis ~/.kesl/<Anwendungsversion>/ksn_license.<ID der Sprache>. Wenn Sie die Verwendung von Kaspersky Security Network ablehnen, wird der Update-Vorgang von Kaspersky Endpoint Security nicht unterbrochen. Sie können den Modus von Kaspersky Security Network später aktivieren, deaktivieren oder ändern.

Wenn Sie in 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.

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

So aktualisieren Sie die Anwendung:

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

   - Für ein Paket im RPM-Format:

     ```
     # [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] rpm -U --replacefiles --replacepkgs kesl-12.4.0-<Build-Nummer>.<arch>.rpm [kesl-gui-12.4.0-<Build-Nummer>.<arch>.rpm]
     ```

wobei <arch> der Architektur entspricht:

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

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

- Für ein Paket im DEB-Format:

  `# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] apt-get install ./kesl_12.4.0-<Build-Nummer>_<arch>.deb [./kesl-gui_12.4.0-<Build-Nummer>_<arch>.deb]`

  wobei <arch> der Architektur entspricht:

  - i386 – für 32-Bit-Betriebssysteme
  - amd64 – für 64-Bit-Betriebssysteme
  - arm64 – für 64-Bit-Betriebssysteme mit ARM-Architektur

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

2. Kaspersky Endpoint Security wird automatisch neu gestartet.

Beispiel:
Aktualisieren des Anwendungspakets im RPM-Format mit dem Paket der grafischen Benutzeroberflächen für 64-Bit-Betriebssysteme*:*

```
# KESL_EULA_AGREED=yes KESL_PRIVACY_POLICY_AGREED=yes KESL_USE_KSN=yes rpm -U --replacefiles --replacepkgs kesl-12.4.0-<Build-Nummer>.x86_64.rpm kesl-gui-12.4.0-<Build-Nummer>.x86_64.rpm
```

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

Änderungen an den Anwendungseinstellungen, die Sie nach Abschluss der Aktualisierung und vor dem Neustart der Anwendung vornehmen, werden nicht gespeichert.

Besonderheiten beim Festlegen von Parameterwerten während eines Updates der Anwendung

Wenn Sie die Anwendung über die Verwaltungskonsole von Kaspersky Security Center verwalten, können Sie Richtlinien und Aufgaben konvertieren, um für die Richtlinien- und Aufgabeneinstellungen die Werte zu verwenden, die in der vorhergehenden Version der Anwendung konfiguriert wurden (Details s. Hilfe zu Kaspersky Security Center). Das Verfahren zum Konvertieren von Richtlinien und Aufgaben ist in der Kaspersky Security Center Web Console nicht verfügbar.

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.

Update-Quellen der Datenbanken

In der neuen Version der Anwendungen haben sich die Aufgaben zum Aktualisieren der Datenbanken wie folgt geändert:

- Der Parameter **Kaspersky-Update-Server verwenden, wenn keine anderen Update-Quellen verfügbar sind** (`UseKLServersWhenUnavailable`) wurde gelöscht. Sie können diese Funktionalität anhand anderer Aufgabenparameter konfigurieren.

- Sie können gleichzeitig mehrere Update-Quellen für zur Aktualisierung der Datenbanken angeben. Die App verwendet diese Update-Quellen in der Reihenfolge, in der sie in der Quellenliste angezeigt werden.

Nach der Konvertierung von Aufgaben im MMC-Plug-in werden die Update-Quellen wie folgt konfiguriert:

- Wenn in der vorherigen Version **Kaspersky-Update-Server** ausgewählt war, ist in der Liste der Quellen das Kontrollkästchen **Kaspersky-Update-Server** aktiviert.

- Wenn in der vorherigen Version **Kaspersky Security Center** ausgewählt war, ist in der Liste der Quellen das Kontrollkästchen **Kaspersky Security Center** aktiviert.

  Wenn in der vorherigen Version zusätzlich das Kontrollkästchen **Kaspersky-Update-Server verwenden, wenn keine anderen Update-Quellen verfügbar sind** aktiviert war, ist in der Liste der Quellen zusätzlich das Kontrollkästchen **Kaspersky-Update-Server** aktiviert und die Quelle **Kaspersky Security Center** wird in die erste Zeile der Liste verschoben.

- Wenn in der vorherigen Version eine benutzerdefinierte Quelle (Option **Andere Quellen im lokalen oder globalen Netzwerk**) konfiguriert war, wird zur Liste der Quellen die benutzerdefinierte Quelle mit ihrem Parameter (Pfad oder Webadresse der Quelle) hinzugefügt und deren Kontrollkästchen aktiviert.

  Wenn in der vorherigen Version zusätzlich das Kontrollkästchen **Kaspersky-Update-Server verwenden, wenn keine anderen Update-Quellen verfügbar sind** aktiviert war, ist in der Liste der Quellen zusätzlich das Kontrollkästchen **Kaspersky-Update-Server** aktiviert und die benutzerdefinierte Quelle wird in die erste Zeile der Liste verschoben.

Vom Web-Plug-in wird das Konvertieren von Richtlinien nicht unterstützt.

Nach dem Update der Anwendung über die Befehlszeile werden die Update-Quellen wie folgt konfiguriert:

- Wenn in der vorherigen Version für den Parameter `SourceType` der Wert `KLServers` ausgewählt war, wird im Abschnitt **[Sources]** folgende Update-Quelle erstellt: `SourceType=KLServers`, `Enabled=Yes`.
- Wenn in der vorherigen Version für den Parameter `SourceType` der Wert `SCServer` ausgewählt war, wird im Abschnitt **[Sources]** folgende Update-Quelle erstellt: `SourceType=SCServer`, `Enabled=Yes`.

  Wenn in der vorherigen Version zusätzlich der Parameterwert `UseKLServersWhenUnavailable=Yes` festgelegt war, wird im Abschnitt **[Sources]** folgende zweite Update-Quelle erstellt: `SourceType=KLServers`, `Enabled=Yes`.
- Wenn in der vorherigen Version `SourceType` auf `Custom` festgelegt war und die benutzerdefinierte Quelle im Abschnitt **[CustomSources.item_#]** konfiguriert war, wird im Abschnitt **[Sources]** eine benutzerdefinierte Update-Quelle erstellt: `SourceType=Custom`, `URL=<Pfad oder Webadresse der Quelle>`, `Enabled=Yes`.

  Wenn in der vorherigen Version zusätzlich der Parameterwert `UseKLServersWhenUnavailable=Yes` festgelegt war, wird im Abschnitt **[Sources]** folgende zweite Update-Quelle erstellt: `SourceType=KLServers`, `Enabled=Yes`.

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.

Vom Web-Plug-in wird das Konvertieren von Richtlinien nicht unterstützt.

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

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.

Vom Web-Plug-in wird das Konvertieren von Richtlinien nicht unterstützt.

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 der Parameter `UseKSN=Basic/Extended` eingestellt ist und vor dem Update der Wert `CloudMode=Yes` angegeben war.

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

- Wenn Sie ein MMC- oder Web-Plug-in verwenden, wählen Sie die Option **Erweiterter KSN-Modus** und aktivieren Sie das Kontrollkästchen **Cloud-Modus aktivieren**.
- Wenn Sie die Befehlszeile verwenden, legen Sie für den Parameter `UseKSN` den Wert `Basic` oder `Extended` und für den Parameter `CloudMode` den Wert `Yes` fest.

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.

Vom Web-Plug-in wird das Konvertieren von Richtlinien nicht unterstützt.

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 `UseKSN=Basic/Extended` nach dem Update festgelegt wurde und `UseMDR=Yes` vor dem Update festgelegt 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.

Anwendung deinstallieren

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

1. **Deinstallation der Anwendung und der grafischen Oberfläche.**

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

   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:

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

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

2. **Administrationsagent deinstallieren**

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

   Sie können den Administrationsagenten auf folgende Arten deinstallieren:

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

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

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

Nach der Deinstallation der Anwendung werden alle Informationen gelöscht, die während ihrer Ausführung gespeichert wurden, mit Ausnahme der Lizenzdatenbank. Es werden zudem die installierten Zertifikate der Anwendung gelöscht. Die Lizenzdatenbank bleibt erhalten und Sie können sie für eine erneute Installation der Anwendung verwenden. Die eindeutige ID der Programminstallation (SensorID) wird ebenfalls gespeichert.

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

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

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

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

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

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

Anwendung über die Befehlszeile löschen

Anwendungspaket und Paket der grafischen Benutzeroberfläche deinstallieren

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

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

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

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

Anwendungspaket ohne Paket der grafischen Oberfläche deinstallieren

Um die Anwendung nach einer Installation aus einem RPM-Paket ohne Deinstallation der grafischen Oberfläche der Anwendung zu deinstallieren, führen Sie den folgenden Befehl aus:

```
# rpm -e kesl
```

Um die Anwendung nach einer Installation aus einem DEB-Paket ohne Deinstallation der grafischen Oberfläche der Anwendung zu deinstallieren, führen Sie den folgenden Befehl aus:

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

Paket der grafischen Oberfläche deinstallieren

Um die grafische Oberfläche der Anwendung nach einer Installation aus einem RPM-Paket zu deinstallieren, führen Sie den folgenden Befehl aus:

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

Um die grafische Oberfläche der Anwendung nach einer Installation aus einem DEB-Paket zu deinstallieren, führen Sie den folgenden Befehl aus:

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

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

Administrationsagent über die Befehlszeile deinstallieren

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

```
# rpm -e klnagent
```

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

```
# rpm -e klnagent64
```

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

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

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

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

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

Deinstallation der Verwaltungs-Plug-ins für Kaspersky Endpoint Security

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

So entfernen Sie das MMC-Plug-in für die Verwaltung von 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**.

Lizenzierung der Anwendung

Dieser Abschnitt enthält Informationen zu den grundlegenden Konzepten der Lizenzierung von Kaspersky-Anwendungen sowie Informationen über die Besonderheiten bei der Aktivierung der Anwendung "Kaspersky Endpoint Security".

Nach der Aktivierung der Anwendung wird es empfohlen, die Gültigkeitsdauer der von der Anwendung verwendeten Lizenz zu überwachen. Auf diese Weise kann die Lizenz bei Bedarf rechtzeitig verlängert werden. Das Anzeigen von Informationen zu den Lizenzschlüsseln, die von Kaspersky Endpoint Security verwendetet werden, ist sowohl in Kaspersky Security Center als auch über die Befehlszeile auf einem geschützten Gerät möglich.

Über den 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 zum Text des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie bestätigen, akzeptieren Sie die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie. Wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags oder der Datenschutzrichtlinie nicht akzeptieren, müssen Sie die Installation des Programms abbrechen und dürfen das Programm nicht verwenden.

- 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>.

Über die Lizenz

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

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

Es sind folgende Lizenztypen vorgesehen:

- *Testversion*

  Kostenlose Lizenz zum Testen des Programms. Die Testlizenz besitzt eine beschränkte Gültigkeitsdauer.

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

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

- *Kommerziell*

  Kostenpflichtige Lizenz.

  Nach Ablauf der kommerziellen Lizenz stellt die Anwendung 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.

  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 Aktivierung von Kaspersky Endpoint Security ist eine Lizenz erforderlich, von der die grundlegenden Funktionen der Anwendung abgedeckt werden. Eine Hauptlizenz kann auch zusätzliche Funktionen der Anwendung abdecken (z. B. Funktionen zur Integration mit den Detection and Response-Lösungen von Kaspersky). Wenn die Hauptlizenz, unter der Sie die Anwendung verwenden, die erforderlichen zusätzlichen Funktionen nicht enthält, müssen Sie eine separate Lizenz erwerben, um die zusätzlichen Funktionen zu aktivieren.

Für weitere Informationen über den in der Hauptlizenz und in der Lizenz für zusätzliche Funktionen enthaltenen Funktionsumfang wenden Sie sich bitte an den Kaspersky-Partner, bei dem Sie die Lizenz erworben haben.

Über das Lizenzzertifikat

Das *Lizenzzertifikat* ist ein Dokument, das Sie zusammen mit der Schlüsseldatei oder dem Aktivierungscode erhalten.

Das Lizenzzertifikat enthält folgende Informationen über die vorliegende Lizenz:

- Lizenz-ID oder Bestellnummer.
- Informationen über den Benutzer, für den die Lizenz ausgestellt wurde
- Informationen über das Programm, das mit der ausgestellten Lizenz aktiviert werden kann
- quantitative Beschränkungen im Hinblick auf die Lizenzierungseinheiten (beispielsweise Geräte, auf denen das Programm mit dieser Lizenz verwendet werden darf)
- Datum für den Beginn der Lizenzgültigkeit
- Ablaufdatum der Lizenz oder Gültigkeitsdauer der Lizenz
- Lizenztyp

Über den 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.

Um die Anwendung zu aktivieren, benötigen Sie einen Haupt-Lizenzschlüssel. Wenn von der Hauptlizenz, unter der Sie die Anwendung verwenden, die erforderlichen zusätzlichen Funktionen nicht abgedeckt werden (z. B. die Funktionen von Kaspersky Endpoint Detection and Response Optimum), benötigen Sie auch einen Lizenzschlüssel für die zusätzlichen Funktionen.

Sie können auf eine der folgenden Arten einen Lizenzschlüssel auf dem geschützten Gerät hinzufügen: indem Sie eine *Schlüsseldatei* anwenden oder einen *Aktivierungscode* eingeben. Sobald Sie einen Lizenzschlüssel auf dem geschützten Gerät hinzufügen, wird er in der Oberfläche der Anwendung als eindeutige Folge aus Buchstaben und Ziffern angezeigt.

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

Ein Lizenzschlüssel kann als aktiver Schlüssel oder als Reserveschlüssel hinzugefügt werden.

- *Aktiver Lizenzschlüssel* – Ein Lizenzschlüssel, der aktuell für die Ausführung der App verwendet wird. Als aktive Schlüssel können hinzugefügt werden: Schlüssel für Testlizenzen, Schlüssel für kommerzielle Lizenzen (kommerzieller Schlüssel) oder Schlüssel für Abonnements. Es kann nur ein Schlüssel als aktiver Schlüssel hinzugefügt werden. Für zusätzliche Funktionen können mehrere aktive Lizenzschlüssel hinterlegt sein.

- *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.

  Um die Gültigkeitsdauer der Hauptlizenz der Anwendung zu verlängern, können Sie einen Reserveschlüssel für die grundlegenden Funktionen hinzufügen. Wenn Sie zusätzliche Funktionen unter einer separaten Lizenz aktiviert haben, können Sie auch einen Reserveschlüssel für die zusätzlichen Funktionen hinzufügen.

  Ein Reserveschlüssel kann nur hinzugefügt werden, wenn bereits ein aktiver Lizenzschlüssel vom gleichen Typ vorhanden ist.

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

Über den Aktivierungscode

Ein *Aktivierungscode* ist eine einmalige Sequenz aus zwanzig lateinischen Buchstaben und Ziffern. Wenn Sie den Aktivierungscode eingeben, wird ein Lizenzschlüssel hinzugefügt, der Kaspersky Endpoint Security aktiviert. Der Aktivierungscode wird an die E-Mail-Adresse geschickt, die Sie angegeben haben, nachdem Sie Kaspersky Endpoint Security gekauft oder eine Testversion von Kaspersky Endpoint Security angefordert haben.

Um 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 Anwendung setzen Sie sich bitte mit dem Partner von Kaspersky in Verbindung, von dem Sie die Lizenz erworben haben.

Über die Schlüsseldatei

Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung "key", die Sie von Kaspersky erhalten. Mit der Schlüsseldatei wird ein Lizenzschlüssel für die Programmaktivierung hinzugefügt.

Die Schlüsseldatei wird an Ihre angegebene E-Mail-Adresse gesendet, nachdem Sie Kaspersky Endpoint Security gekauft oder nachdem Sie die Testversion von Kaspersky Endpoint Security bestellt haben.

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

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

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

- Kontaktieren Sie den Lizenzverkäufer.
- Auf der Kaspersky-Website mithilfe des vorhandenen Aktivierungscodes eine Schlüsseldatei anfordern.

Über das Abonnement

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

Es gibt beschränkte (z. B. auf ein Jahr) und unbefristete (ohne Ablaufdatum) Abos. Damit die Anwendung nach Ablauf des beschränkten Abonnements weiter funktioniert, müssen Sie Ihr Abonnement verlängern. Ein unbefristetes Abonnement wird automatisch verlängert, wenn die Gebühren des Händlers rechtzeitig bezahlt wurden.

Nach Ablauf eines befristeten Abonnements kann Ihnen eine Übergangsfrist zur Verlängerung des Abonnements angeboten werden. Während dieses Zeitraums behält das Programm seine Funktionalität bei. Ob es eine Nachfrist gibt und wie lang diese ist, wird vom Dienstanbieter bestimmt.

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

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

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

Vergleich der Anwendungsfunktionen je nach Lizenz

Der Umfang der verfügbaren Funktionen von "Kaspersky Endpoint Security" hängt von der Art der Hauptlizenz ab.

Eine Hauptlizenz, unter der die Anwendung genutzt wird, kann sowohl grundlegende als auch zusätzliche Funktionen der Anwendung umfassen. So können z. B. mit der Lizenz "Kaspersky Optimum Security" sowohl die grundlegenden Schutz- und Kontrollkomponenten als auch die Funktionen zur Integration von Kaspersky Endpoint Detection and Response Optimum aktiviert werden.

Um zusätzliche Funktionen der Anwendung zu aktivieren, können auch separate Lizenzen verwendet werden, etwa eine Lizenz zur Aktivierung der Funktionen von Kaspersky Unified Monitoring and Analysis Platform.

Für weitere Informationen über den in der Hauptlizenz und in der Lizenz für zusätzliche Funktionen enthaltenen Funktionsumfang wenden Sie sich bitte an den Kaspersky-Partner, bei dem Sie die Lizenz erworben haben.

Liste der Funktionen öffnen, die unter der Haupt-Lizenz der Anwendung verfügbar sind

Anwendung aktivieren und Lizenzschlüssel verwalten

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

Um Kaspersky Endpoint Security auf einem geschützten Gerät zu aktivieren, müssen Sie der Anwendung einen Hauptlizenzschlüssel hinzufügen. Wenn von der Hauptlizenz, unter der Sie die Anwendung verwenden, die erforderlichen zusätzlichen Funktionen von Kaspersky Endpoint Security nicht abgedeckt werden, müssen Sie der Anwendung auch einen Lizenzschlüssel für die zusätzlichen Funktionen hinzufügen:

- Einen separaten Lizenzschlüssel des Typs "Kaspersky Endpoint Detection and Response Optimum Add-on" (im Folgenden auch "EDR Optimum-Schlüssel" genannt), um die Komponente EDR-Optimum zu aktivieren.
- Einen separaten Lizenzschlüssel des Typs "Kaspersky Unified Monitoring and Analysis Platform Add-on" (im Folgenden auch "KUMA-Schlüssel" genannt), um die Funktionen der Kaspersky Unified Monitoring and Analysis Platform zu aktivieren.

- Einen separaten Lizenzschlüssel des Typs "Kaspersky Managed Detection and Response Optimum/Expert Add-on" (im Folgenden auch "MDR-Schlüssel" genannt), um die Komponente MDR zu aktivieren.
- Einen separaten Lizenzschlüssel des Typs "Kaspersky Endpoint Detection and Response Expert (on-premise) Add-on" (im Folgenden auch "Schlüssel von EDR Expert (on-premise)" genannt), um die EDR Expert (on-premise) zu aktivieren.

Der Schlüssel für EDR Expert (on-premise) wird auch zur Aktivierung der Anwendung "Kaspersky Endpoint Security" im Modus als Endpoint Detection and Response Agent verwendet. In diesem Modus muss der Anwendung kein Haupt-Lizenzschlüssel hinzugefügt werden.

Sie können der Anwendung einen Lizenzschlüssel auf eine der folgenden Arten hinzufügen:

- mittels Schlüsseldatei
- mittels Aktivierungscode

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, ist eine Aktivierung der Anwendung nicht notwendig. Sie aktivieren Kaspersky Security for Virtualization Light Agent. Die Aktivierung erfolgt auf der Seite des Schutzservers (dies ist eine Komponente von Kaspersky Security for Virtualization Light Agent) durch das Hinzufügen eines Lizenzschlüssels auf der SVM. Bei Bedarf kann einer SVM auch ein Lizenzschlüssel zur Aktivierung zusätzlicher Funktionen hinzugefügt werden.

Wenn Sie die Anwendung "Kaspersky Endpoint Security" während der Installation nicht aktiviert haben (durch das Hinzufügen eines Schlüssels zum Installationspaket oder durch Ausführen der Erstkonfiguration), müssen Sie die installierte Anwendung auf eine der folgenden Arten aktivieren:

- Remote, über Kaspersky Security Center:
  - Durch Verwendung der Aufgabe für das Hinzufügen eines Schlüssels zur Anwendung.
  - Durch Verteilung eines Lizenzschlüssels, der sich auf dem Administrationsserver befindet, an die Client-Geräte.
- Über die Befehlszeile mithilfe von Verwaltungsbefehlen.

Sie haben außerdem folgende Möglichkeiten, um der Anwendung einen Lizenzschlüssel für zusätzliche Funktionen hinzuzufügen: unter Verwendung der Aufgabe zum Hinzufügen eines Schlüssels, mittels des Vorgangs zum Verteilen des Schlüssels an Client-Geräte oder mithilfe der Befehle zur Verwaltung von Lizenzschlüsseln. Das Hinzufügen eines Schlüssels für zusätzliche Funktionen unterscheidet sich nicht vom Hinzufügen des Hauptlizenzschlüssels der Anwendung.

Wenn die Anwendung "Kaspersky Endpoint Security" im Standard-Modus verwendet wird, kann der Schlüssel für die zusätzlichen Funktionen erst hinzugefügt werden, wenn der Haupt-Lizenzschlüssel der Anwendung bereits hinzugefügt wurde.

Sie können der Anwendung auch einen Reserveschlüssel für die grundlegenden Funktionen der Anwendung und einen Reserveschlüssel für zusätzliche Funktionen hinzufügen. Der Reserveschlüssel wird aktiv, sobald die an den aktiven Schlüssel gebundene gültige Lizenz abläuft oder der aktive Schlüssel gelöscht wird. Ein Reserveschlüssel verhindert, dass nach Ablauf der Lizenz die Funktionalität der Anwendung eingeschränkt wird.

Ein Reserveschlüssel kann nur hinzugefügt werden, wenn bereits ein aktiver Lizenzschlüssel hinzugefügt wurde.

Das Anzeigen von Informationen zu den Lizenzschlüsseln, die von der Anwendung verwendetet werden, ist sowohl remote in Kaspersky Security Center als auch über die Befehlszeile auf einem geschützten Gerät möglich.

Sie können auch über die grafische Oberfläche die Anwendung aktivieren und die Lizenzschlüssel verwalten.

App über Kaspersky Security Center aktivieren

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

- Durch Verwendung der Aufgabe für das Hinzufügen eines Schlüssels zur Anwendung.

  Mittels dieser Methode können Sie einen Lizenzschlüssel zum jeweiligen Gerät oder zu Geräten hinzufügen, die zur Administrationsgruppe gehören. Beim Erstellen einer Aufgabe wird jener Schlüssel verwendet, der zum Schlüsselspeicher von Kaspersky Security Center hinzugefügt wurde. Das Hinzufügen eines Lizenzschlüssels zum Schlüsselspeicher ist vor oder während dem Erstellen einer Aufgabe möglich.

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

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

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

Schlüssel über die Kaspersky Security Center Web Console hinzufügen

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

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

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

   - Geben Sie den Aktivierungscode ein und klicken Sie auf **Senden**.
   - Klicken Sie auf die Schaltfläche **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 einen Schlüssel hinzu, indem Sie die Aufgabe zum Hinzufügen eines Schlüssels verwenden:

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

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Konfigurieren Sie die Aufgabeneinstellungen:

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

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

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

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

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

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

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

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

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

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

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

- Geben Sie den Aktivierungscode ein und klicken Sie auf **Senden**.
- Klicken Sie auf die Schaltfläche **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. Schließen Sie den Assistenten ab.

   Eine neue Aufgabe wird in der Liste mit Aufgaben angezeigt.

9. Aktivieren Sie das Kontrollkästchen neben der Aufgabe. Klicken Sie auf **Starten**.

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

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

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

1. Wählen Sie im Hauptfenster von Web Console die Option **Vorgänge → Lizenzen für Kaspersky-Software**.

2. Öffnen Sie die Schlüssel-Einstellungen über den Link mit dem Namen der 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.

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**.

Besonderheiten bei der Aktivierung in Kaspersky Security Center Cloud Console

Für die Kaspersky Security Center Cloud Console ist eine Testversion verfügbar. *Testversion* – Eine spezielle Version der Kaspersky Security Center Cloud Console, mit der Benutzer die Funktionen der Cloud Console kennenlernen können. In dieser Version können Sie über einen Zeitraum von 30 Tagen Aktionen in einem Arbeitsbereich ausführen. Alle verwalteten Anwendungen einschließlich 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. Nähere Informationen über die Cloud Console finden Sie in der Dokumentation zu Kaspersky Security Center Cloud Console.

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

Lizenzschlüsselverwaltung über die Befehlszeile

Um die Lizenzschlüssel auf einem Gerät zu verwalten, können Sie die Befehle zur Verwaltung von Lizenzschlüsseln verwenden.

Befehle zur Verwaltung von Lizenzschlüsseln können nur ausgeführt werden, wenn die Anwendung im Standard-Modus oder im Modus als Endpoint Detection and Response Agent verwendet wird. Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, schlagen die Befehle zur Verwaltung von Lizenzschlüsseln mit einem Fehler fehl. Sie aktivieren die Anwendung als Teil der Lösung Kaspersky Security for Virtualization Light Agent; Sie müssen die Anwendung nicht separat aktivieren.

Um der Anwendung einen aktiven Lizenzschlüssel hinzuzufügen, führen Sie diesen Befehl aus:

```
kesl-control [-L] --add-active-key <Pfad zur Schlüsseldatei/Aktivierungscode>
```

wobei:

- `Pfad der Schlüsseldatei` – Pfad der Schlüsseldatei. Wenn sich die Schlüsseldatei im aktuellen Verzeichnis befindet, ist die Angabe des Dateinamens ausreichend.
- `Aktivierungscode` – Aktivierungscode.

Um der Anwendung einen Reserve-Lizenzschlüssel hinzuzufügen, führen Sie diesen Befehl aus:

```
kesl-control [-L] --add-reserve-key <Pfad zur Schlüsseldatei/Aktivierungscode>
```

Wenn der Anwendung auf dem Gerät noch kein aktiver Schlüssel hinzugefügt wurde, schlägt der Befehl fehl.

Mit dem Befehl zum Hinzufügen eines Schlüssels können Sie sowohl Haupt-Lizenzschlüssel für die Anwendung als auch für Lizenzschlüssel für zusätzliche Funktionen hinzufügen. Der Schlüsseltyp muss nicht im Befehl angeben werden.

Für das Löschen eines Haupt-Lizenzschlüssels und das Löschen von Schlüsseln für zusätzliche Funktionen existieren unterschiedliche Befehle.

Um den aktiven Hauptschlüssel zu löschen, führen Sie diesen Befehl aus:

```
kesl-control [-L] --remove-active-key
```

Um den Reserveschlüssel des Hauptschlüssel zu löschen, führen Sie diesen Befehl aus:

```
kesl-control [-L] --remove-reserve-key
```

Um den aktiven EDR Optimum-Schlüssel zu löschen, führen Sie diesen Befehl aus:

```
kesl-control [-L] --remove-active-key --edr-optimum
```

Um den Reserveschlüssel für EDR Optimum zu löschen, führen Sie diesen Befehl aus:

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

Um den aktiven KUMA-Schlüssel zu entfernen, führen Sie den folgenden Befehl aus:

```
kesl-control [-L] --remove-active-key --kuma
```

Um den Reserveschlüssel für KUMA zu löschen, führen Sie diesen Befehl aus:

```
kesl-control [-L] --remove-reserve-key --kuma
```

Um den aktiven MDR-Schlüssel zu entfernen, führen Sie den folgenden Befehl aus:

```
kesl-control [-L] --remove-active-key --mdr
```

Um den Reserveschlüssel für MDR zu löschen, führen Sie diesen Befehl aus:

```
kesl-control [-L] --remove-reserve-key --mdr
```

Um den aktiven Schlüssel von EDR Expert (on-premise) zu löschen, führen Sie diesen Befehl aus:

```
kesl-control [-L] --remove-active-key --edr-kata
```

Um den Reserveschlüssel von EDR Expert (on-premise) zu löschen, führen Sie diesen Befehl aus:

```
kesl-control [-L] --remove-reserve-key --edr-kata
```

Informationen zu den verwendeten Lizenzschlüsseln anzeigen

Sie können Informationen zu den von Kaspersky Endpoint Security verwendeten Lizenzschlüsseln auf folgende Weise anzeigen:

- Im Kaspersky Security Center in den Eigenschaften der Aufgabe Schlüssel hinzufügen.

  Die Eigenschaften der Aufgabe *Schlüssel hinzufügen* werden Informationen über den Schlüssel angezeigt, welcher der Anwendung nach Ausführung dieser Aufgabe hinzugefügt wird.

- In Kaspersky Security Center in den Eigenschaften der auf dem Client-Gerät installierten Kaspersky-Anwendungen.

  Auf einem geschützten Gerät werden in den Eigenschaften der Anwendung "Kaspersky Endpoint Security" Informationen über den aktiven Schlüssel und den Reserveschlüssel angezeigt, die der Anwendung auf diesem Gerät hinzugefügt wurden. Sie können die Anwendungseinstellungen sowohl über die Web Console als auch über die Verwaltungskonsole anzeigen.

- In Kaspersky Security Center im Bericht über die Lizenzschlüsselnutzung.

  Sie können den Bericht über die Schlüsselnutzung sowohl über die Web Console (**Überwachung und Berichterstattung** → **Berichte**) als auch 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.

- Im Lizenzschlüsselspeicher von Kaspersky Security Center.

  Sie können den Schlüsselspeicher sowohl über die Web Console (**Vorgänge** → **Lizenzen von Kaspersky**) als auch über die Verwaltungskonsole (Ordner **Lizenzen von Kaspersky**) öffnen. Der Speicher zeigt Informationen zu allen Schlüsseln an, die dem Kaspersky Security Center Administrationsserver hinzugefügt wurden.

- Auf einem Gerät mit installiertem Kaspersky Endpoint Security. Sie können Informationen über die von Kaspersky Endpoint Security verwendete Lizenz über die Befehlszeile anzeigen.

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.

Wenn Sie Kaspersky Endpoint Security im Standard-Modus oder im Modus als Endpoint Detection and Response Agent ausführen und Kaspersky Security Center zur Verwaltung dieser Anwendung verwenden, werden die Informationen über das Hinzufügen und Entfernen von Lizenzschlüsseln sowie über die Gültigkeitsdauer der Lizenz standardmäßig im Protokoll des Betriebssystems aufgezeichnet.

Informationen zu den Schlüsseln auf einem Gerät über die Web Console anzeigen

So zeigen Sie in der Web Console Informationen zu Lizenzschlüsseln an, die einem Gerät hinzugefügt wurden:

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

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** oberhalb der Liste der verwalteten Geräte und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

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

3. Suchen Sie in der Liste das Gerät, für das Sie Informationen anzeigen möchten, und klicken Sie auf den Gerätenamen.

4. 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. Öffnen Sie in dem neuen Fenster mit den Anwendungseinstellungen auf der Registerkarte **Allgemein** den Abschnitt **Lizenzen**.

   Der Abschnitt enthält Informationen über die der Anwendung hinzugefügten Lizenzschlüssel und über die mit diesen Schlüsseln verknüpften Lizenzen:

   - **Lizenzschlüsselstatus** – Status des Schlüssels: 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

Informationen zu den Schlüsseln auf einem Gerät über die Verwaltungskonsole anzeigen

So zeigen Sie in der Verwaltungskonsole von Kaspersky Security Center Informationen zu Lizenzschlüsseln an, die einem Gerät hinzugefügt wurden:

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.
   - Die **Gültigkeitsdauer der Lizenz** ist die Anzahl der Tage, die bis zum Ende der Nutzungsdauer des Programms verbleiben, welches vorher durch das Hinzufügen dieses Schlüssels aktiviert wurde.
   - **Lizenzbeschränkung** – Anzahl der Geräte, auf denen der Schlüssel verwendet werden kann.
   - **Aktivierungsdatum** (dieses Feld ist nur für den aktiven Schlüssel verfügbar) – Datum des Hinzufügens des aktiven Schlüssels.
   - **Gültigkeitsdauer** (dieses Feld ist nur für den aktiven Schlüssel verfügbar) – Ende der Nutzungsdauer der Anwendung, welche durch das Hinzufügen eines aktiven Schlüssels aktiviert wurde.

Lizenz- und Schlüsselinformationen über die Befehlszeile anzeigen

Über die Befehlszeile können Sie mit dem Befehl `-L --query` Informationen über den der Anwendung hinzugefügten aktiven Lizenzschlüssel und den Reserve-Lizenzschlüssel sowie die Lizenz anzeigen, mit der die Anwendung aktiviert wurde. Wenn der Anwendung ein separater Schlüssel zum Aktivieren zusätzlicher Funktionen hinzugefügt wurde, werden auch Informationen über hinzugefügte aktive Lizenzschlüssel und Reserve-Lizenzschlüssel für zusätzliche Funktionen angezeigt.

Um Informationen über Lizenzschlüssel und Lizenzen auf einem Gerät anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control -L --query [--json]
```

Wobei gilt: `--json` – Gibt Daten im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

- Informationen über den aktiven Haupt-Lizenzschlüssel, sofern dieser hinzugefügt wurde:
  - Das Datum und die Uhrzeit des Ablaufs der Gültigkeitsdauer der Lizenz, mit der die Anwendung verwendet wird.
  - Die Anzahl der Tage bis zum Ablauf der Gültigkeitsdauer der Lizenz.
  - Informationen zu Einschränkungen der Schutzfunktionen.
  - Informationen zu Einschränkungen der Funktion zum Update der Anwendungsdatenbanken.
  - 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 über den Reserveschlüssel für den Haupt-Lizenzschlüssel: Wird angezeigt, wenn die Anwendung im Standard-Modus verwendet wird und ein Reserveschlüssel hinzugefügt wurde. Wenn das Programm im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, werden Informationen zum Reserveschlüssel nicht angezeigt; der Reserveschlüssel wird der SVM hinzugefügt.
    - Das Datum und die Uhrzeit des Ablaufs der Gültigkeitsdauer der Lizenz, mit der die Anwendung verwendet wird.
    - Informationen zu Einschränkungen der Schutzfunktionen.
    - Informationen zu Einschränkungen der Funktion zum Update der Anwendungsdatenbanken.
    - 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 über den aktiven Schlüssel für zusätzliche Funktionen, sofern ein separater Schlüssel hinzugefügt wurde:
    - Zeitpunkt des Ablaufs der Lizenz zur Aktivierung zusätzlicher Funktionen.
    - Die Anzahl der Tage bis zum Ablauf der Gültigkeitsdauer der Lizenz.
    - Informationen zu Einschränkungen der Funktion zum Update der Anwendungsdatenbanken.
    - 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 über den Reserveschlüssel für zusätzliche Funktionen. Wird angezeigt, wenn die Anwendung im Standard-Modus oder im Modus als Endpoint Detection and Response Agent verwendet wird und ein Reserveschlüssel für die zusätzlichen Funktionen hinzugefügt wurde. Wenn das Programm im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, werden Informationen zum Reserveschlüssel nicht angezeigt; der Reserveschlüssel wird der SVM hinzugefügt.

  - Zeitpunkt des Ablaufs der Lizenz zur Aktivierung zusätzlicher Funktionen.
  - Informationen zu Einschränkungen der Funktion zum Update der Anwendungsdatenbanken.
  - 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.

Das Abrufen von Informationen über die Lizenz, unter der die Anwendung verwendet wird, ist auch mit dem Befehl zum Anzeigen der Informationen zur Anwendungsausführung möglich: `kesl-control --app-info`.

Bereitstellung von Daten

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

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

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

Daten, die bei Verwendung eines Aktivierungscodes bereitgestellt werden

Wenn Kaspersky Endpoint Security im Standard-Modus oder im Modus als Endpoint Detection and Response Agent verwendet wird und mit einem Aktivierungscode aktiviert wurde, stimmen Sie zu, die folgenden Informationen automatisch an Kaspersky zu übertragen, damit die rechtmäßige Nutzung der Anwendung bestätigt werden kann und Statistikdaten zur Verteilung und Verwendung der Anwendung 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 ist
- ID der gültigen Lizenz
- Datum und Uhrzeit der Erstellung des Lizenzschlüssels der Anwendung
- Datum und Uhrzeit auf dem Benutzergerät;
- Datum und Uhrzeit des Ablaufs der Lizenz zur Verwendung der Anwendung
- 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 Modus als Endpoint Detection and Response Agent 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 Anwendung abgerufen werden können:

- von der Lizenz abgeleitete Anwendungs-ID
- vollständige Version der Anwendung
- ID der Anwendungslizenz
- Typ der verwendeten Lizenz
- ID der Anwendungsinstallation (PCID)
- ID des Starts des Updates der Anwendung
- verarbeitete Webadresse

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

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

- Zur Aktivierung übermittelt die Kaspersky Endpoint Security folgende Daten an den Schutzserver: die Gültigkeitsdauer der Statusbestätigung des Lizenzschlüssels: die BIOS-ID der geschützten virtuellen Maschine; Informationen über die Lizenz, die der Light Agent für seine Ausführung benötigt.
- 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 Anwendung:
    - 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 von KSN im erweiterten Modus während der Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise)

Wenn Sie Kaspersky Endpoint Security als Teil von Kaspersky Endpoint Detection and Response Expert (on-premise) 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 Basismodus 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:
  - Name des Prozesses
  - Argumente des Prozesses
  - Pfad zur ausführbaren Datei des Prozesses
  - Prozess-ID (PID)
  - ID des übergeordneten Prozesses (PPID)
  - Name des Benutzers, der den Prozess gestartet hat
  - Datum und Uhrzeit des Starts des Prozesses

- Informationen über Dienste:
  - Name des Dienstes
  - Beschreibung des Dienstes
  - Pfad und Name der ausführbaren Datei des Dienstes
  - ID des Dienstes
  - Typ des Dienstes (Kernel-Treiber, Adapter usw.)
  - Status des Dienstes
  - Startmodus des Dienstes
  - Name des Benutzers, unter dem der Dienst gestartet wurde
- Informationen über das Dateisystem:
  - Name der Partition
  - Buchstabe der Partition
  - Typ der Partition
- Informationen über das Betriebssystem:
  - Name und Version des Betriebssystems
  - Netzwerkname des geschützten Geräts
  - Domäne oder Gruppe, der das Gerät zugehörig ist
- Informationen über Web-Aktivitäten:
  - Name des Browsers
  - Version des Browsers
  - Zeitpunkt des letzten Zugriffs auf eine Webressource
  - Web-Adresse der HTTP-Anfrage
  - Name des Benutzers, der die HTTP-Anfrage gestellt hat
  - Name des Prozesses, der die HTTP-Anfrage gestellt hat
  - Pfad zur ausführbaren Datei des Prozesses, der die HTTP-Anfrage gestellt hat
  - ID des Prozesses, der die HTTP-Anfrage gestellt hat
  - Webadresse der Quelle der HTTP-Anfrage
  - Webadresse der angeforderten Ressource

- Benutzeragent zur Verarbeitung von Webanfragen (HTTP User-Agent)
- Ausführungszeit der HTTP-Anfrage
- Die eindeutige Kennung des Prozesses, der die HTTP-Anfrage gestellt hat.

Daten zum Aufbau der Entwicklungskette der Bedrohung

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

- Allgemeine Informationen zum dem Alarm:
  - Datum und Uhrzeit des Alarms
  - Objektname
  - Untersuchungsmodus
  - Status der letzten Aktivität mit Bezug auf den Alarm
  - Grund für eine fehlgeschlagene Verarbeitung des Alarms
- Informationen zum verarbeiteten Objekt:
  - ID des Prozesses
  - ID des übergeordneten Prozesses (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, von der die Datei heruntergeladen wurde
- MD5- und SHA256-Hashsummen der Anwendung, von der die Datei heruntergeladen wurde
- Name der Anwendung, von der die Datei das letzte Mal geändert wurde
- MD5- und SHA256-Hashsummen der Anwendung, von der die Datei das letzte Mal geändert wurde
- Anzahl der Starts des verarbeiteten Objekts
- Datum und Uhrzeit des ersten Starts des Objekts
- Eindeutige Datei-ID
- Vollständiger Name der Datei (lokale Datei oder Webadresse)
- Webadresse der verarbeiteten Webanfrage
- Quelle der Links der verarbeiteten Webanfrage (HTTP-Referer)
- Benutzeragent der verarbeiteten Webanfrage
- Typ der verarbeiteten Webanfrage (GET oder POST)
- Lokaler IP-Port für die verarbeitete Webanfrage
- Remote-IP-Port der verarbeiteten Webanfrage
- Richtung der Verbindung für die verarbeiteten Webanfrage (eingehend oder ausgehend)
- ID des Prozesses, in den der Schadcode eingeschleust wurde

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 der Parameter
  - 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
  - Status, mit denen die Aufgaben abgeschlossen wurden
  - 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
  - Dateien, die vom Server angefordert wurden
  - 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
    - Dateiattribute
    - Datum und Uhrzeit der Datei-Erstellung
    - Datum und Uhrzeit der letzten Datei-Änderung
    - MD5- und SHA256-Hashes 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
    - Datum und Uhrzeit des Starts des Prozesses
    - 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 der Anwendung "Kaspersky Endpoint Security" mit der Lösung "Kaspersky Endpoint Detection and Response Expert (on-premise)" speichert Kaspersky Endpoint Security die folgenden Informationen, die persönliche und vertrauliche Daten enthalten können:

- Adressen der Server, welche die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) gewährleisten.
- Öffentlichen Schlüssel vom Zertifikat des Servers, der die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) gewährleistet.
- 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 die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) gewährleistet, sowie Parameter für die Datenübertragung an den Server.

- Status der Verbindung mit dem Server, der die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) gewährleistet, sowie Informationen über Fehler des Client- und Server-Zertifikats.
- Parameter der Aufgaben, die von den Servern erhalten werden, welche die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) gewährleisten:
  - Einstellungen des Zeitplans für den Aufgabenstart
  - Namen und Kennwörter der Benutzerkonten, unter denen die Aufgaben ausgeführt werden sollen
  - Versionen der Parameter
  - 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 einer Integration der Anwendung "Kaspersky Endpoint Security" mit der Lösung "Kaspersky Endpoint Detection and Response Expert (on-premise)" kann die Anwendung folgenden Daten speichern und an den Server weiterleiten, der die Integration gewährleistet:

- 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
  - Status, mit denen die Aufgaben abgeschlossen wurden
  - 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
  - Dateien, die vom Server angefordert wurden
  - 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:
    - Name des Prozesses
    - 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:
    - Name des Prozesses
    - 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
    - Dateiattribute
    - Datum und Uhrzeit der Datei-Erstellung
    - Datum und Uhrzeit der letzten Datei-Änderung
    - MD5- und SHA256-Hashes 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
  - Datum und Uhrzeit des Starts des Prozesses
  - 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 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
- 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
  - Datum und Uhrzeit des Starts des Prozesses
  - 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

Konzept der Anwendungsverwaltung

Zur Verwaltung von Kaspersky Endpoint Security können Sie Folgendes verwenden:

- Kaspersky Security Center
- Befehlszeile
- Grafische Oberfläche der Anwendung

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

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

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

Anwendung 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.

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-Plug-in für die Verwaltung für die MMC-basierte Verwaltungskonsole (im Folgenden auch "MMC-Plug-in" genannt) bereitgestellt.

- 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. Kaspersky Security Center Web Console kann im Browser eines jeden Geräts, welches Zugriff auf den Administrationsserver hat, aufgerufen werden.

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

- 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 Anwendungsverwaltung mit Kaspersky Security Center Cloud Console ist nicht verfügbar, wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen 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.

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).

Wenn die App im EDR-Agent-Modus verwendet wird, ist nur eine begrenzte Auswahl an App-Komponenten 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“.

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

Über die Verwaltungs-Plug-ins für Kaspersky Endpoint Security

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

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

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

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

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

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

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

Wenn in der Kaspersky Security Center Web Console Version 16.0 oder 16.1 die Web-Plug-ins für Kaspersky Endpoint Security für Windows (Build 12.11.0.2004) und Kaspersky Endpoint Security für Linux (Build 12.4.0.1354) installiert sind, kann es beim Update des Web-Plug-ins für Kaspersky Endpoint Security für Windows auf Version 12.11.0.6004 zu einer Störung der Richtlinie von Kaspersky Endpoint Security für Linux kommen. Wechseln Sie in diesem Fall zum Fenster **Einstellungen** → **Web-Plug-ins** und löschen Sie die Web-Plug-ins von Kaspersky Endpoint Security für Windows, Kaspersky Endpoint Security für Linux und des Unified Protection and Management Plug-ins. Installieren Sie dann zuerst das Web-Plug-in für Kaspersky Endpoint Security für Linux und anschließend das Web-Plug-in für Kaspersky Endpoint Security für Windows.

Über die Richtlinien von Kaspersky Security Center

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

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

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

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

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

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

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

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

Für einige Listen können Sie die Vereinigung der Listenelemente aktivieren. Gehen Sie wie folgt vor, um Listenelemente zusammenzuführen:

- Aktivieren Sie in den Eigenschaften der untergeordneten Richtlinie auf der Registerkarte **Allgemein** die Option **Einstellungen der übergeordneten Richtlinie vererben**.

- 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.

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

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.

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.

Wenn die Anwendung zum Zeitpunkt des Löschens der Richtlinie nicht gestartet ist, wird die Richtlinie nach dem Start der Anwendung weiterhin auf dem Gerät angewendet. Die Anwendung wird in diesem Fall weiterhin mit den in der Richtlinie angegebenen Einstellungen ausgeführt.

Weitere Informationen zu Richtlinien und Richtlinienprofilen sowie zum Mechanismus der Einstellungsvererbung finden Sie in der Hilfe zu Kaspersky Security Center.

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

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

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

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

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

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

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

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

- *Schadsoftware-Untersuchung*. Während der Ausführung dieser Aufgabe untersucht die Anwendung die in den Aufgabeneinstellungen angegebenen Bereiche des Geräts auf Viren und andere Schadsoftware.
- *Untersuchung wichtiger Bereiche*. Während der Ausführung dieser Aufgabe untersucht die Anwendung die Bootsektoren, die Autostart-Objekte, den Prozess-Speicher und den Kernelspeicher.
- *Untersuchung von Containern*. Während der Ausführung dieser Aufgabe untersucht die Anwendung Container und Images auf Viren und andere Schadsoftware.
- *Inventarisierung*. Während der Ausführung dieser Aufgabe ruft die Anwendung Informationen über alle ausführbaren Dateien der Anwendung ab, die auf den Geräten gespeichert sind.
- *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.

Die Auswahl von Einstellungen sowie die Standardwerte der Aufgaben sind abhängig vom Typ der Lizenz. Die Aufgaben *Schlüssel hinzufügen, Update* und *Rollback des Datenbanken-Updates* sind nicht anwendbar, wenn die Anwendung im Light Agent-Modus verwendet 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.

Richtlinienverwaltung in der Web Console

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

- Richtlinie erstellen
- Richtlinieneinstellungen ändern Sie können Richtlinieneinstellungen auf der Registerkarte **Anwendungseinstellungen** im Fenster der Richtlinieneigenschaften konfigurieren. Die Parameter der Richtlinie in der Web Console werden in Anhang 5 beschrieben.

  > Wenn das Benutzerkonto, mit dem der Zugriff auf den Administrationsserver erfolgt, nicht zum Ändern von Einstellungen einzelner Funktionsbereiche berechtigt ist, können die Einstellungen dieser Funktionsbereiche nicht bearbeitet werden.

- Richtlinieneinstellungen exportieren und importieren

  > Der Export und Import der Richtlinieneinstellungen von Kaspersky Endpoint Security 12.3 für Linux nach Kaspersky Endpoint Security 12.4 für Linux wird nicht unterstützt.

- Richtlinie kopieren und verschieben
- Richtlinie löschen
- Status der Richtlinie ändern
- Richtlinienprofile erstellen

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

Richtlinienerstellung in der Web Console

So erstellen Sie eine Richtlinie in der Web Console:

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

   Die Liste mit Richtlinien und Richtlinienprofilen wird geöffnet.

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

3. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Richtlinien wird gestartet.

4. Wählen Sie im 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:

   - 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.

6. Wenn Sie die Anwendung im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, konfigurieren Sie die Einstellungen zur SVM-Ermittlung:

   a. Wählen Sie die Methode aus, die von den Light Agents verwendet werden soll, um für verfügbare SVMs zum Herstellen einer Verbindung zu erkennen:

      - **Integrationsserver verwenden**

        Wenn diese Option ausgewählt ist, stellt der Light Agent eine Verbindung zum Integrationsserver her, um eine Liste der für die Verbindung verfügbaren SVMs und Informationen darüber zu erhalten.

      - **Manuell eingegebene Liste mit SVM-Adressen verwenden**

        Wenn diese Option ausgewählt ist, können Sie eine Liste von SVMs angeben, mit denen Light Agents, die durch diese Richtlinie verwaltet werden, eine Verbindung herstellen können. Die Light Agents stellen nur Verbindungen zu den in der Liste angegebenen SVMs her.

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

   b. Wenn Sie "Integrationsserver verwenden" ausgewählt haben, werden im Fenster des Assistenten die aktuellen Verbindungsparameter der Light Agents mit dem Integrationsserver angezeigt: Adresse und Port für die Verbindung. Bei Bedarf können Sie neue Verbindungsparameter angeben:

      a. Klicken Sie auf die Schaltfläche **Konfigurieren** und geben Sie im neuen Fenster die neuen Verbindungsparameter an:

         - **Adresse**

IP-Adresse im IPv4-Format oder als vollqualifizierter Domänenname (FQDN) des Geräts mit installiertem Integrationsserver. Wenn als Adresse 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 **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 **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 "Manuell angegebene Liste mit SVM-Adressen verwenden" ausgewählt haben, zeigt das Fenster eine Liste der SVMs an, mit denen Light Agents, die von dieser Richtlinie verwaltet werden, eine Verbindung herstellen können. Um eine SVM zur Liste hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie im angezeigten Fenster die IP-Adresse im IPv4-Format oder den vollqualifizierten Domänennamen (FQDN) der SVM an. Sie können 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 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. Das Fenster mit den Einstellungen der neuen Richtlinie wird geöffnet; die Registerkarte **Allgemein** ist darin ausgewählt. Geben Sie einen Namen der neuen Richtlinie ein.

   Sie können außerdem die folgenden Einstellungen der Richtlinie konfigurieren:

   - Richtlinienstatus:

     - **Aktiv**. Die aktuell auf das Gerät angewendete Richtlinie. Wenn diese Option ausgewählt ist, wird diese Richtlinie bei der nächsten Synchronisierung des Geräts mit dem Administrationsserver auf dem Gerät aktiv. Diese Option ist standardmäßig ausgewählt.

     - **Inaktiv**. 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 erben**. 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.

     - **Vererben der Einstellungen für untergeordnete 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 erben** 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 den Richtlinieneinstellungen finden Sie in der Dokumentation zu Kaspersky Security Center.

9. Wenn Sie andere Richtlinieneinstellungen konfigurieren möchten, wechseln Sie zur Registerkarte **Anwendungseinstellungen** und nehmen Sie die erforderlichen Änderungen vor.

   Die Richtlinieneinstellungen können auch zu einem späteren Zeitpunkt angepasst werden.

10. Klicken Sie auf **Speichern**.

Die erstellte Richtlinie erscheint in der Liste mit Richtlinien.

Allgemeine Informationen über die Verwaltung von Richtlinien finden Sie in der Hilfe zu Kaspersky Security Center.

Richtlinieneinstellungen in der Web Console ändern

So ändern Sie Richtlinieneinstellungen in der Web Console:

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

   Die Liste mit Richtlinien wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, welche die Geräte enthält, auf jene die Richtlinie angewendet wird. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

   In der Liste werden die Richtlinien angezeigt, die für die ausgewählte Administrationsgruppe konfiguriert sind.

3. Klicken Sie in der Liste auf den Namen der erforderlichen Richtlinie.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.

4. Ändern Sie die Richtlinieneinstellungen auf der Registerkarte **Anwendungseinstellungen**.

5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die Richtlinie wird mit den aktualisierten Einstellungen gespeichert.

Richtlinieneinstellungen in der Web Console

Die Auswahl von Einstellungen sowie die Standardwerte der Richtlinieneinstellungen sind abhängig von der Lizenz, mit der die Anwendung aktiviert wurde. Je nachdem, in welchem Modus die Anwendung verwendet wird, werden einige Richtlinieneinstellungen möglicherweise auf die Anwendung angewendet oder nicht.

Sie können Richtlinieneinstellungen auf der Registerkarte **Anwendungseinstellungen** im Fenster der Richtlinieneigenschaften konfigurieren.

Die Parameter der Richtlinie in der Web Console werden in Anhang 5 beschrieben.

Abschnitt	Unterabschnitte
Host-Schutz	**Schutz vor bedrohlichen Dateien**. In diesem Unterabschnitt können Sie den Schutz vor bedrohlichen Dateien verwalten. **Schutz vor BadUSB-Angriffen**. In diesem Unterabschnitt können Sie die Parameter des Schutzes vor BadUSB-Angriffen konfigurieren. **Untersuchung von Wechseldatenträgern**. In diesem Unterabschnitt können Sie die Parameter der Untersuchung von Wechseldatenträgern bei Anschluss an ein geschütztes Gerät konfigurieren. **Verhaltensanalyse**. In diesem Unterabschnitt können Sie die Parameter der Verhaltensanalyse der Anwendung konfigurieren. **Schutz vor Verschlüsselung**. In diesem Unterabschnitt können Sie die Parameter des Schutzes vor bösartiger Remote-Verschlüsselung konfigurieren. **Exploit-Prävention**. In diesem Unterabschnitt können Sie die Parameter der Exploit-Prävention konfigurieren.
Kommunikations- und Web-Schutz	**Schutz vor E-Mail-Bedrohungen**. In diesem Unterabschnitt können Sie die Parameter des Schutzes vor E-Mail-Bedrohungen konfigurieren. **Schutz vor Web-Bedrohungen**. In diesem Unterabschnitt können Sie die Parameter des Schutzes vor Web-Bedrohungen konfigurieren. **Schutz vor Netzwerkbedrohungen**. In diesem Unterabschnitt können Sie die Parameter des Schutzes vor Netzwerkbedrohungen konfigurieren. **Firewall**. In diesem Unterabschnitt können Sie die Parameter der Firewall-Verwaltung konfigurieren.
Sicherheitskontrolle	**Gerätekontrolle**. In diesem Unterabschnitt können Sie die Parameter der Gerätekontrolle konfigurieren. **Web-Kontrolle**. In diesem Unterabschnitt können Sie die Parameter der Web-Kontrolle konfigurieren. **App-Kontrolle**. In diesem Unterabschnitt können Sie die Parameter der Programmkontrolle konfigurieren. **Überwachung der Systemintegrität**. In diesem Unterabschnitt können Sie die Parameter der Überwachung der Systemintegrität konfigurieren.
Vertrauenswürdige Zone	In diesem Abschnitt können Sie die folgenden Parameter konfigurieren: • Ausnahmen, die für die Komponente Schutz vor bedrohlichen Dateien gelten. • Ausnahmen, die für die Komponente Schutz vor Web-Bedrohungen gelten. • Ausnahmen, die für die Komponente Schutz vor Netzwerkbedrohungen gelten. • Ausnahmen von der Untersuchung des Netzwerkverkehrs. • Ausschließen von Mount-Punkten vom Abfangen von Dateioperationen. • Vertrauenswürdige Geräte, die von der Gerätekontrolle berücksichtigt werden.

Abschnitt	Unterabschnitte
Allgemeine Einstellungen	**Erkennungseinstellungen**. In diesem Unterabschnitt können Sie die folgenden Einstellungen verwalten: • Erkennung legaler Programme, die von Angreifern zur Beschädigung von Geräten oder Daten ausgenutzt werden können. • Modus des Modul zum Abfangen von Dateioperationen. **Kaspersky Security Network**. In diesem Unterabschnitt können Sie die Verwendung von Kaspersky Security Network in Kaspersky Endpoint Security konfigurieren. **Interaktion mit dem Benutzer**. In diesem Unterabschnitt können Sie die folgenden Einstellungen verwalten: • Starteinstellungen der Anwendung. • Berechtigungen der Benutzer zur Verwaltung von Aufgaben. **Performance**. In diesem Unterabschnitt können Sie die folgenden Einstellungen verwalten: • Abbrechen geplanter Aufgaben auf einem Gerät, das im Akkubetrieb läuft. • Prozess-Speicher von der Untersuchung ausschließen. • Begrenzung der Nutzung von Speicher- und CPU-Ressourcen für Untersuchungsaufgaben. • Begrenzung des von der Anwendung verwendeten residenten Speichers. • Überwachung der Anwendungsstabilität. **Netzwerkeinstellungen**. In diesem Unterabschnitt können Sie: • Proxyserver-Einstellungen, wenn Benutzer von Client-Geräten über einen Proxyserver auf das Internet zugreifen. • Einstellungen der Untersuchung des Netzwerkdatenverkehrs. **Untersuchung von Containern**. In diesem Unterabschnitt können Sie die Ausführung der Komponente zur Überwachung von Containern konfigurieren. **Technischer Support**. In diesem Unterabschnitt können Sie die Optionen für die Protokollierung und Dump-Erstellung konfigurieren. **Reports and Storage**. In diesem Unterabschnitt können Sie die Einstellungen für das Backup und die Quarantäne konfigurieren. **KSC-Integration**. In diesem Unterabschnitt können Sie die Einstellungen für das Übertragen von Informationen an den Speicher von Kaspersky Security Center konfigurieren. **Konfiguration der Kommunikation mit dem Betriebssystem**. In diesem Unterabschnitt können Sie: • Den Mechanismus auswählen, den die Anwendung zum **Abfangen von Systemereignissen** verwenden soll. In der Web Console können Sie das Abfangen von Systemereignissen in den Richtlinieneigenschaften (**Programmeinstellungen → Allgemeine Einstellungen → Einstellungen für die Interaktion mit dem Betriebssystem**) konfigurieren. Die Parameter werden nur auf Geräten angewendet, deren Betriebssystem die fanotify-Technologie unterstützt. • Zusätzliche Parameter für die Erfassung von Telemetriedaten konfigurieren. **Benachrichtigungseinstellungen**. In diesem Unterabschnitt können Sie die Parameter der Benachrichtigungseinstellungen konfigurieren.
Konfiguration der integrierten Agenten	**Managed Detection and Response**. In diesem Unterabschnitt können Sie die Integration mit Kaspersky Managed Detection and Response aktivieren und deaktivieren und die für die Integration erforderliche MDR-BLOB-Datei hochladen. **Network Detection and Response (KATA)**. In diesem Unterabschnitt können Sie die Integration mit Kaspersky Network Detection and Response (KATA) aktivieren und deaktivieren. **Endpoint Detection and Response**. In diesem Unterabschnitt können Sie die Integration mit Kaspersky Detection and Response Optimum aktivieren und deaktivieren sowie die Integrationseinstellungen konfigurieren. **Endpoint Detection and Response Expert (on-premise)**. In diesem Unterabschnitt können Sie die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder Kaspersky Endpoint Detection and Response (KATA) aktivieren oder deaktivieren sowie die Integrationseinstellungen konfigurieren. **Sandbox**. In diesem Unterabschnitt können Sie die Integration mit Sandbox aktivieren und deaktivieren sowie die Integrationseinstellungen konfigurieren. **KUMA-Integration**. In diesem Unterabschnitt können Sie die Integration mit der Kaspersky Unified Monitoring and Analysis Platform aktivieren und deaktivieren sowie die Integrationseinstellungen konfigurieren.

Abschnitt	Unterabschnitte
Light Agent-Modus Die Einstellungen in diesem Abschnitt können nur angewendet werden, wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird.	**SVM discovery settings**. In diesem Unterabschnitt können Sie die Methode auswählen, die von den Light Agents verwendet werden soll, um verfügbare SVMs zum Herstellen einer Verbindung zu erkennen: **Konfiguration der Verbindung mit dem Integrationsserver**. In diesem Unterabschnitt können Sie für die Light-Agent-Komponente von Kaspersky Security for Virtualization die Verbindung der Light Agents zum Integrationsserver konfigurieren. **SVM connection tag**. In diesem Unterabschnitt können Sie dem Light Agent die Verwendung von Tags ermöglichen und ein Tag zuweisen, das der Light Agent für die Verbindung verwendet. **SVM selection algorithm**. In diesem Unterabschnitt können Sie festlegen, welchen Algorithmus die Light Agents zur SVM-Auswahl verwenden sollen. **Connection protection**. In diesem Unterabschnitt können Sie die Verschlüsselung für den Kanal zur Datenübertragung zwischen dem Light Agent und dem Schutzserver aktivieren.

Richtlinien in der Verwaltungskonsole verwalten

In der Kaspersky Security Center Verwaltungskonsole können Sie folgende Aktionen für Richtlinien ausführen:

- Eine Richtlinie erstellen
- Richtlinieneinstellungen bearbeiten Sie können Richtlinieneinstellungen im Fenster der Richtlinieneigenschaften konfigurieren.

  Wenn das Benutzerkonto, mit dem der Zugriff auf den Administrationsserver erfolgt, nicht zum Ändern von Einstellungen einzelner Funktionsbereiche berechtigt ist, können die Einstellungen dieser Funktionsbereiche nicht bearbeitet werden.

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

Allgemeine Informationen über die Verwaltung von Richtlinien finden Sie in der Hilfe zu Kaspersky Security Center.

Richtlinien mithilfe der Verwaltungskonsole erstellen

So erstellen Sie eine Richtlinie in der Verwaltungskonsole:

1. Wählen Sie in der Struktur der Verwaltungskonsole im Ordner **Verwaltete Geräte** die Administrationsgruppe aus, 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 Anwendung im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, konfigurieren Sie die Einstellungen zur SVM-Ermittlung:

   a. Wählen Sie die Methode aus, die von den Light Agents verwendet werden soll, um für verfügbare SVMs zum Herstellen einer Verbindung zu erkennen:

      - **Integrationsserver verwenden**

        Wenn diese Option ausgewählt ist, stellt der Light Agent eine Verbindung zum Integrationsserver her, um eine Liste der für die Verbindung verfügbaren SVMs und Informationen darüber zu erhalten.

- **Manuell eingegebene Liste mit SVM-Adressen verwenden**

  Wenn diese Option ausgewählt ist, können Sie eine Liste von SVMs angeben, mit denen Light Agents, die durch diese Richtlinie verwaltet werden, eine Verbindung herstellen können. Die Light Agents stellen nur Verbindungen zu den in der Liste angegebenen SVMs her.

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

b. Wenn Sie "Integrationsserver verwenden" ausgewählt haben, werden im Fenster des Assistenten die aktuellen Verbindungsparameter der Light Agents mit dem Integrationsserver angezeigt: Adresse und Port für die Verbindung. Bei Bedarf können Sie neue Verbindungsparameter angeben:

   a. Klicken Sie auf die Schaltfläche **Ändern** und geben Sie im neuen Fenster die neuen Verbindungsparameter an:

      - **Adresse**

        IP-Adresse im IPv4-Format oder als vollqualifizierter Domänenname (FQDN) des Geräts mit installiertem Integrationsserver.

        Wenn das Gerät mit installierter Kaspersky Security Center Verwaltungskonsole zu einer Domäne gehört, wird in dem Feld standardmäßig der Domänenname des Geräts angegeben.

        Wenn das Gerät mit installierter Kaspersky Security Center Verwaltungskonsole in keiner Domäne enthalten ist oder der Integrationsserver auf einem anderen Gerät installiert ist, muss das Feld manuell ausgefüllt werden.

        Wenn als Adresse 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 "Manuell angegebene Liste mit SVM-Adressen verwenden" ausgewählt haben, zeigt das Fenster eine Liste der SVMs an, mit denen Light Agents, die von dieser Richtlinie verwaltet werden, eine Verbindung herstellen können. Um eine SVM zur Liste hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie im angezeigten Fenster die IP-Adresse im IPv4-Format oder den vollqualifizierten Domänennamen (FQDN) der SVM an. Sie können 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. Diese Option ist standardmäßig ausgewählt.

    - **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.

Die Richtlinieneinstellungen können zu einem späteren Zeitpunkt angepasst werden. Allgemeine Informationen über die Verwaltung von Richtlinien finden Sie in der Dokumentation zu Kaspersky Security Center.

Richtlinieneinstellungen in der Kaspersky Security Center Verwaltungskonsole ändern

So ändern Sie Richtlinieneinstellungen in der Verwaltungskonsole:

1. Öffnen Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu der die erforderlichen Geräte gehören.
2. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
3. Wählen Sie in der Liste der Richtlinien die erforderliche Richtlinie aus und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>** mit einem Doppelklick.

   Sie können das Fenster mit den Richtlinieneigenschaften auch über den Eintrag **Eigenschaften** im Kontextmenü der Richtlinie oder durch Klicken auf den Link **Richtlinieneinstellungen konfigurieren** rechts neben der Liste der Richtlinien im Block mit den Richtlinieneinstellungen öffnen.
4. Passen Sie die Richtlinieneinstellungen an.
5. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf **OK**, um die Änderungen zu speichern.

Richtlinieneinstellungen in der Verwaltungskonsole

Die Auswahl von Einstellungen sowie die Standardwerte der Richtlinieneinstellungen sind abhängig von der Lizenz, mit der die Anwendung aktiviert wurde. Je nachdem, in welchem Modus die Anwendung verwendet wird, werden einige Richtlinieneinstellungen möglicherweise auf die Anwendung angewendet oder nicht.

Sie können Richtlinieneinstellungen in Abschnitten und Unterabschnitten im Fenster der Richtlinieneigenschaften konfigurieren. Informationen über die Konfiguration der allgemeinen Richtlinien- und Ereigniseinstellungen finden Sie in der Dokumentation zu Kaspersky Security Center.

Abschnitt	Unterabschnitte
Basisschutz	**Schutz vor bedrohlichen Dateien**. In diesem Unterabschnitt können Sie den Schutz vor bedrohlichen Dateien verwalten. **Ausschlüsse aus dem Schutz vor bedrohlichen Dateien**. In diesem Unterabschnitt können Sie die Ausnahmen konfigurieren, die beim Schutz vor bedrohlichen Dateien angewendet werden. **Firewall-Verwaltung**. In diesem Unterabschnitt können Sie die Parameter der Firewall-Verwaltung konfigurieren. **Schutz vor Web-Bedrohungen**. In diesem Unterabschnitt können Sie die Parameter des Schutzes vor Web-Bedrohungen konfigurieren. **Schutz vor E-Mail-Bedrohungen**. In diesem Unterabschnitt können Sie die Parameter des Schutzes vor E-Mail-Bedrohungen konfigurieren. **Schutz vor Netzwerkbedrohungen**. In diesem Unterabschnitt können Sie die Parameter des Schutzes vor Netzwerkbedrohungen konfigurieren. **Schutz vor BadUSB-Angriffen**. In diesem Unterabschnitt können Sie die Parameter des Schutzes vor BadUSB-Angriffen konfigurieren.
Erweiterter Schutz	**Kaspersky Security Network**. In diesem Unterabschnitt können Sie die Verwendung von Kaspersky Security Network in Kaspersky Endpoint Security konfigurieren. **Schutz vor Verschlüsselung**. In diesem Unterabschnitt können Sie die Parameter des Schutzes vor bösartiger Remote-Verschlüsselung konfigurieren. **Verhaltensanalyse**. In diesem Unterabschnitt können Sie die Parameter der Verhaltensanalyse der Anwendung konfigurieren.
Detection and Response	**Managed Detection and Response**. In diesem Unterabschnitt können Sie die Integration mit Kaspersky Managed Detection and Response aktivieren und deaktivieren und die für die Integration erforderliche MDR-BLOB-Datei hochladen. **EDR Expert (on-premise)**. In diesem Unterabschnitt können Sie die Integration mit Kaspersky Endpoint Detection and Response (KATA) aktivieren und deaktivieren sowie die Integrationseinstellungen konfigurieren. **Network Detection and Response (KATA)**. In diesem Unterabschnitt können Sie die Integration mit Kaspersky Network Detection and Response (KATA) aktivieren und deaktivieren.
Sicherheitskontrolle	**Programmkontrolle**. In diesem Unterabschnitt können Sie die Parameter der Programmkontrolle konfigurieren. **Überwachung der System-Integrität**. In diesem Unterabschnitt können Sie die Parameter der Überwachung der Systemintegrität konfigurieren. **Gerätekontrolle**. In diesem Unterabschnitt können Sie die Parameter der Gerätekontrolle konfigurieren. **Web-Kontrolle**. In diesem Unterabschnitt können Sie die Parameter der Web-Kontrolle konfigurieren.
Lokale Aufgaben	**Aufgabenverwaltung**. In diesem Unterabschnitt können Sie die Benutzerberechtigungen für die Aufgabenverwaltung konfigurieren. **Untersuchung von Wechseldatenträgern**. In diesem Unterabschnitt können Sie die Parameter der Untersuchung von Wechseldatenträgern bei Anschluss an ein geschütztes Gerät konfigurieren.

Abschnitt	Unterabschnitte
Allgemeine Einstellungen	**Proxyserver-Einstellungen**. In diesem Unterabschnitt können Sie die Proxyserver-Einstellungen konfigurieren, wenn Benutzer von Client-Geräten über einen Proxyserver auf das Internet zugreifen. **Anwendungseinstellungen**. In diesem Unterabschnitt können Sie die folgenden Einstellungen verwalten: • Erkennung legaler Programme, die von Angreifern zur Beschädigung von Geräten oder Daten ausgenutzt werden können. • Benachrichtigungseinstellungen. • Begrenzung der Nutzung von Speicher- und CPU-Ressourcen für Untersuchungsaufgaben. • Begrenzung der Anzahl benutzerdefinierter Untersuchungsaufgaben, die ein nicht privilegierter Benutzer auf einem Gerät gleichzeitig ausführen kann. • Starteinstellungen der Anwendung. • Einstellungen zur Erstellung von Protokollen und Dumps. • Überwachung der Anwendungsstabilität. • Begrenzung des von der Anwendung verwendeten residenten Speichers. • Modus des Modul zum Abfangen von Dateioperationen. **Einstellungen der Untersuchung von Containern**. In diesem Unterabschnitt können Sie die Ausführung der Komponente zur Überwachung von Containern konfigurieren. **Netzwerkeinstellungen** In diesem Unterabschnitt können Sie die Einstellungen für die Untersuchung des Netzwerkverkehrs konfigurieren. **Globale Ausschlüsse**. In diesem Unterabschnitt können Sie: • Ausschließen von Mount-Punkten vom Abfangen von Dateioperationen. • Ausnahmen für industrielle Software: Ausschlüsse nach Prozessen, Dateien und Verzeichnissen, die mit Software eines bestimmten Typs verbunden sind. **Prozess-Speicher von der Untersuchung ausschließen**. In diesem Unterabschnitt können Sie Ausnahmen für Prozess-Speicher bei der Untersuchung konfigurieren. **Speichereinstellungen**. In diesem Unterabschnitt können Sie: • Einstellungen für das Backup und die Quarantäne. • Einstellungen zur Übertragung von Informationen an den Kaspersky Security Center. **Einstellungen für die Interaktion mit dem Betriebssystem** In diesem Unterabschnitt können Sie Folgendes konfigurieren: • Den Mechanismus auswählen, den die Anwendung zum Abfangen von Systemereignissen verwenden soll. • Zusätzliche Parameter für die Erfassung von Telemetriedaten konfigurieren.
Integration mit KUMA	**Integration mit KUMA**. In diesem Unterabschnitt können Sie die Integration mit der Kaspersky Unified Monitoring and Analysis Platform aktivieren und deaktivieren sowie die Integrationseinstellungen konfigurieren.
Light Agent-Modus Die Einstellungen in diesem Abschnitt können nur angewendet werden, wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird.	**Verbindung mit dem Integrationsserver**. In diesem Unterabschnitt können Sie für die Light-Agent-Komponente von Kaspersky Security for Virtualization die Verbindung der Light Agents zum Integrationsserver konfigurieren. **Konfiguration der SVM-Erkennung**. In diesem Unterabschnitt können Sie die Methode auswählen, die von den Light Agents verwendet werden soll, um verfügbare SVMs zum Herstellen einer Verbindung zu erkennen: **Tag für die Verbindung zur SVM**. In diesem Unterabschnitt können Sie dem Light Agent die Verwendung von Tags ermöglichen und ein Tag zuweisen, das der Light Agent für die Verbindung verwendet. **Algorithmus der SVM-Auswahl**. In diesem Unterabschnitt können Sie festlegen, welchen Algorithmus die Light Agents zur SVM-Auswahl verwenden sollen. **Schutz der Verbindung**. In diesem Unterabschnitt können Sie die Verschlüsselung für den Kanal zur Datenübertragung zwischen dem Light Agent und dem Schutzserver aktivieren.

Aufgabenverwaltung in der Web Console

Sie können die folgenden Aktionen für Aufgaben für Kaspersky Endpoint Security in der Web Console ausführen:

- Neue Aufgaben erstellen.
- Aufgabeneinstellungen ändern.

  Wenn das Benutzerkonto, mit dem der Zugriff auf den Administrationsserver erfolgt, nicht zum Ändern von Einstellungen einzelner Funktionsbereiche berechtigt ist, können die Einstellungen dieser Funktionsbereiche nicht bearbeitet werden.

- Ausführung von Aufgaben starten, beenden, anhalten und fortsetzen.

  Die *Update-Aufgabe* kann nicht angehalten oder fortgesetzt werden; sie kann nur gestartet und beendet werden.

- Aufgaben exportieren und importieren.
- Aufgaben löschen.

In der Liste der Aufgaben können Sie die Aufgabenausführung überwachen, indem Sie den Aufgabenstatus und die Statistik zur Aufgabenausführung auf den Geräten anzeigen. Sie können auch eine Auswahl von Ereignissen erstellen, um den Abschluss von Aufgaben zu überwachen (**Überwachung und Berichterstattung** → **Ereignisauswahlen**). Nähere Informationen zur Ereignisauswahl finden Sie in der Dokumentation zu Kaspersky Security Center.

Die Ergebnisse der Aufgabenausführung werden auch lokal auf dem Gerät und in den Berichten von Kaspersky Security Center gespeichert.

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

Wenn das Gerät durch eine Richtlinie verwaltet wird, können in Kaspersky Security Center erstellte Aufgaben möglicherweise nicht über die Befehlszeile oder die grafische Oberfläche der Anwendung angezeigt und verwaltet werden.

Aufgabenerstellung in der Web Console

So erstellen Sie in der Web Console eine Aufgabe für eine Gruppe oder für eine Geräteauswahl:

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 im Hilfesystem von Kaspersky Security Center.

   Wechseln Sie zum nächsten Schritt des Assistenten.

4. Führen Sie abhängig von der ausgewählten Methode zur Definition des Gültigkeitsbereichs der Aufgabe eine der folgenden Aktionen aus:

   - Aktivieren Sie in der Baumstruktur der Administrationsgruppen die Kontrollkästchen neben den erforderlichen Administrationsgruppen.

   - Aktivieren Sie in der Geräteliste die Kontrollkästchen neben den erforderlichen Geräten. Wenn die erforderlichen Geräte nicht in der Liste enthalten sind, können Sie sie auf folgende Weise hinzufügen:

      - Über die Schaltfläche **Geräte hinzufügen**. Sie können Geräte nach Namen oder IP-Adresse hinzufügen, Geräte aus einem bestimmten IP-Bereich hinzufügen oder Geräte aus der Liste der Geräte auswählen, die der Administrationsserver bei der Abfrage des lokalen Unternehmensnetzwerks erkannt hat.

      - Über die Schaltfläche **Geräte aus Datei importieren**. Zum Importieren wird eine TXT-Datei mit einer Liste von Geräteadressen verwendet, wobei jede Adresse in einer separaten Zeile stehen muss.

   - Wählen Sie in der Liste den Namen der Auswahl aus, in der die erforderlichen Geräte enthalten sind.

   Wechseln Sie zum nächsten Schritt des Assistenten.

5. Um die Aufgabeneinstellungen direkt nach der Erstellung zu konfigurieren, aktivieren Sie im letzten Schritt des Assistenten das Kontrollkästchen **Fenster mit den Aufgabeneigenschaften nach der Erstellung öffnen**. Die Aufgabe wird mit Standardeinstellungen erstellt.

6. Schließen Sie den Assistenten ab.

Eine neue Aufgabe wird in der Liste mit Aufgaben 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 auf den Link im Feld **Aktueller Pfad** oberhalb der Liste der verwalteten Geräte und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

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

3. Suchen Sie in der Liste das Gerät, für das Sie 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 direkt nach der Erstellung zu konfigurieren, aktivieren Sie im letzten Schritt des Assistenten das Kontrollkästchen **Fenster mit den Aufgabeneigenschaften nach der Erstellung öffnen**. Die Aufgabe wird mit Standardeinstellungen erstellt.

8. Schließen Sie den Assistenten ab.

Eine neue Aufgabe wird in der Liste mit Aufgaben angezeigt.

Aufgabeneinstellungen in der Web Console ändern

So ändern Sie Aufgabeneinstellungen in der Web Console:

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

   Die Aufgabenliste wird geöffnet.

2. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf allen Geräten einer bestimmten Administrationsgruppe ausgeführt wird, klicken Sie auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

     In der Liste werden nur die Aufgaben angezeigt, die für die ausgewählte Administrationsgruppe konfiguriert sind.

- Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf einem oder mehreren Geräten ausgeführt wird (Aufgaben für eine Gerätegruppe), klicken Sie auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster den oberen Knoten mit dem Namen des Administrationsservers.

  In der Liste werden alle auf dem Administrationsserver erstellten Aufgaben angezeigt.

3. Wählen Sie in der Aufgabenliste die erforderliche Aufgabe aus und öffnen Sie über den Link im Aufgabennamen das Fenster mit den Aufgabeneigenschaften.

4. Passen Sie die Einstellungen der Aufgabe an:

   - Auf der Registerkarte **Allgemein** können Sie den Namen der Aufgabe ändern.

   - Auf der Registerkarte **Anwendungseinstellungen** können Sie die spezifischen Aufgabeneinstellungen konfigurieren. Die Verfügbarkeit konfigurierbarer Parameter hängt vom Aufgabentyp ab.

   - Auf der Registerkarte **Zeitplan** können Sie den Zeitplan für den Aufgabenstart und zusätzliche Einstellungen zum Starten und Beenden der Aufgabe konfigurieren.

   Die Registerkarten **Allgemein**, **Ergebnisse**, **Einstellungen**, **Zeitplan** und **Revisionsverlauf** des Eigenschaftenfensters der Aufgabe sind für Kaspersky Security Center vordefiniert. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security Center.

5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Aufgaben in der Web Console starten, beenden, anhalten und fortsetzen

So können Sie eine Aufgabe in der Web Console starten, beenden, anhalten oder fortsetzen:

1. Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console **Assets (Geräte)** → **Aufgaben**.

   Die 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 auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

     In der Liste werden nur die Aufgaben angezeigt, die für die ausgewählte Administrationsgruppe erstellt wurden.

   - Wenn Sie eine Aufgabe starten oder beenden möchten, die auf einem oder mehreren Geräten ausgeführt wird (Aufgabe für eine Gerätegruppe), klicken Sie auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster den oberen Knoten mit dem Namen des Administrationsservers.

     In der Liste werden alle auf dem Administrationsserver erstellten Aufgaben angezeigt.

3. Aktivieren Sie in der Liste der Aufgaben das Kontrollkästchen neben dem Namen der erforderlichen Aufgabe und klicken Sie auf die Schaltfläche für die erforderliche Aktion über der Liste der Aufgaben.

Aufgaben in der Verwaltungskonsole verwalten

Sie können die folgenden Aktionen für Aufgaben für Kaspersky Endpoint Security in der Verwaltungskonsole ausführen:

- Neue Aufgaben erstellen.
- Aufgabeneinstellungen ändern.

  Wenn das Benutzerkonto, mit dem der Zugriff auf den Administrationsserver erfolgt, nicht zum Ändern von Einstellungen einzelner Funktionsbereiche berechtigt ist, können die Einstellungen dieser Funktionsbereiche nicht bearbeitet werden.

- Ausführung von Aufgaben starten, beenden, anhalten und fortsetzen.

  Die *Update-Aufgabe* kann nicht angehalten oder fortgesetzt werden; sie kann nur gestartet und beendet werden.

- Aufgaben exportieren und importieren.
- Aufgaben löschen.

In der Liste der Aufgaben können Sie die Aufgabenausführung überwachen, indem Sie den Aufgabenstatus und die Statistik zur Aufgabenausführung auf den Geräten anzeigen.

Informationen über den Fortschritt und die Ergebnisse der Aufgabenausführung können Sie in der Liste der Ereignisse anzeigen, die Kaspersky Endpoint Security an den Kaspersky Security Center Administrationsserver sendet (auf der Registerkarte **Ereignisse** im Arbeitsbereich des Knotens **Administrationsserver <Servername>**). Sie können auch eine Auswahl von Ereignissen erstellen, um die Ausführung von Aufgaben zu überwachen. Nähere Informationen zur Ereignisauswahl finden Sie in der Dokumentation zu Kaspersky Security Center.

Die Ergebnisse der Aufgabenausführung werden auch lokal auf dem Gerät und in den Berichten von Kaspersky Security Center gespeichert.

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

Wenn das Gerät durch eine Richtlinie verwaltet wird, können in Kaspersky Security Center erstellte Aufgaben möglicherweise nicht über die Befehlszeile oder die grafische Oberfläche der Anwendung angezeigt und verwaltet werden.

Aufgaben in der Verwaltungskonsole erstellen

So erstellen Sie in der Verwaltungskonsole eine Aufgabe für eine Gruppe oder für 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 Einzelheiten finden Sie in der Hilfe zu Kaspersky Security Center).

   b. Führen Sie abhängig von der Methode, die Sie zum Definieren des Gültigkeitsbereichs im angezeigten Fenster angegeben haben, eine der folgenden Aktionen aus:

      - Geben Sie in der Liste der erkannten Geräte die Geräte an, auf denen die Aufgabe ausgeführt werden soll. Aktivieren Sie dazu das Kontrollkästchen in der Liste links neben dem Gerätenamen.

      - Klicken Sie auf die Schaltfläche **Hinzufügen** oder **IP-Bereich hinzufügen** und geben Sie die Geräteadressen manuell an.

      - Klicken Sie auf die Schaltfläche **Importieren** und wählen Sie im angezeigten Fenster eine TXT-Datei mit einer Liste von Geräteadressen aus.

      - Klicken Sie auf die Schaltfläche **Durchsuchen** und geben Sie im angezeigten Fenster den Namen der Auswahl an, 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.

   Eine neue Aufgabe wird in der Liste mit Aufgaben 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.

   Eine neue Aufgabe wird in der Liste mit Aufgaben angezeigt.

Aufgabeneinstellungen in der Verwaltungskonsole ändern

So ändern Sie Aufgabeneinstellungen in der Verwaltungskonsole:

1. Führen Sie in der Verwaltungskonsole eine der folgenden Aktionen aus:

   - Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf Geräten ausgeführt wird, die zu einer bestimmten Administrationsgruppe gehören, wählen Sie diese Administrationsgruppe in der Konsolenstruktur aus und wählen Sie dann im Arbeitsbereich die Registerkarte **Aufgaben** aus.

   - Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf einem oder mehreren Geräten ausgeführt wird (Aufgaben für eine Gerätegruppe), wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.

2. Wählen Sie in der Aufgabenliste die erforderliche Aufgabe aus und öffnen Sie das Fenster **Eigenschaften: <Aufgabenname>** mit einem Doppelklick.

   Sie können das Eigenschaftenfenster der Aufgabe auch über den Eintrag **Eigenschaften** im Kontextmenü der Aufgabe öffnen.

3. Ändern Sie die Einstellungen der Aufgabe. Die Verfügbarkeit konfigurierbarer Parameter hängt vom Aufgabentyp ab.

   Die Registerkarten **Allgemein**, **Benachrichtigungen**, **Zeitplan** und **Revisionsverlauf** des Eigenschaftenfensters der Aufgabe sind für Kaspersky Security Center vordefiniert. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security Center.

4. Klicken Sie im Fenster **Eigenschaften: <Aufgabenname>** auf die Schaltfläche **Übernehmen** oder die Schaltfläche **OK**, um die Änderungen zu speichern.

Aufgaben in der Verwaltungskonsole starten, beenden, anhalten und fortsetzen

So können Sie eine Aufgabe in der Verwaltungskonsole starten, beenden, anhalten oder fortsetzen:

1. Führen Sie in der Verwaltungskonsole eine der folgenden Aktionen aus:

   - Wenn Sie eine Aufgabe starten oder beenden möchten, die auf Geräten ausgeführt wird, die zu einer bestimmten Administrationsgruppe gehören, wählen Sie diese Administrationsgruppe in der Konsolenstruktur aus und wählen Sie dann im Arbeitsbereich die Registerkarte **Aufgaben** aus.

     Die Liste mit den für die ausgewählte Administrationsgruppe erstellten Aufgaben wird geöffnet.

   - Wenn Sie eine Aufgabe starten oder beenden möchten, die auf einem oder mehreren Geräten ausgeführt wird (Aufgaben für eine Gerätegruppe), wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.

     Die Liste mit allen auf dem Administrationsserver erstellten Aufgaben wird geöffnet.

2. Wählen Sie in der Aufgabenliste die erforderliche Aufgabe aus, öffnen Sie das Kontextmenü der Aufgabe und wählen Sie die Aktion aus, die Sie ausführen möchten.

Anwendung über die Befehlszeile verwalten

Über die Befehlszeile können Sie Kaspersky Endpoint Security auf dem Gerät installieren und deinstallieren, starten und beenden sowie die Ausführung der Anwendung lokal verwalten.

Die Ausführung der Funktionskomponenten der Anwendung wird durch *lokale Aufgaben von Kaspersky Endpoint Security* sichergestellt, die im Betriebssystem ausgeführt werden Sie können die Funktionskomponenten der Anwendung auf dem Gerät aktivieren oder deaktivieren, indem Sie Aufgaben von Kaspersky Endpoint Security über die Befehlszeile starten und beenden. Einmalige Untersuchungen des Geräts werden auch durch Starten von Aufgaben für Kaspersky Endpoint Security durchgeführt. Sie können die Ausführungseinstellungen der Funktionskomponenten auf dem Gerät und die Einstellungen für die Untersuchung des Geräts festlegen, indem Sie die *Aufgabeneinstellungen* für Kaspersky Endpoint Security konfigurieren.

Zusätzlich zu den Aufgabeneinstellungen stehen die folgenden Einstellungen zur Konfiguration der Ausführung der Anwendung zur Verfügung:

- Allgemeine Einstellungen der Untersuchung von Containern.
- Einstellungen der Untersuchung des Netzwerkdatenverkehrs.
- Allgemeine Anwendungseinstellungen, welche die Ausführung der Anwendung als Ganzes und die Ausführung einzelner Funktionen bestimmen.

Kaspersky Endpoint Security wird über die Befehlszeile mithilfe der *Verwaltungsbefehle für Kaspersky Endpoint Security* verwaltet.

Wenn die App im EDR-Agent-Modus verwendet wird, ist nur eine begrenzte Auswahl an App-Komponenten 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“.

Aktivieren der automatischen Vervollständigung des kesl-control-Befehls (Bash-Vervollständigung)

Für die Bash-Shell kann die automatische Vervollständigung des Befehls kesl-control aktiviert werden.

Um die automatische Vervollständigung des Befehls kesl-control in der aktuellen Bash-Shell-Sitzung zu aktivieren, führen Sie den folgenden Befehl aus:

```
source /opt/kaspersky/kesl/shared/bash_completion.sh
```

Um die automatische Vervollständigung für alle neuen Bash-Shell-Sitzungen zu aktivieren, führen Sie den folgenden Befehl aus:

```
echo "source /opt/kaspersky/kesl/shared/bash_completion.sh" >> ~/.bashrc
```

Aufgabenverwaltung über die Befehlszeile

Zur Verwaltung von Kaspersky Endpoint Security über die Befehlszeile sind die folgenden Anwendungsaufgaben vorgesehen:

- *Schutz vor bedrohlichen Dateien*. Mit dieser Aufgabe können Sie den Echtzeitschutz vor bedrohlichen Dateien aktivieren und deaktivieren und Einstellungen für die Komponente "Schutz vor bedrohlichen Dateien" definieren. Die Aufgabe startet automatisch, wenn die App gestartet wird.

- *Schadsoftware-Untersuchung*. Mit dieser Aufgabe können Sie Objekte des Dateisystems auf Befehl auf Schadsoftware untersuchen und Einstellungen für die Untersuchung definieren. Mit dieser Aufgabe können Sie eine vollständige oder benutzerdefinierte Untersuchung des Geräts durchführen.

- *Untersuchung wichtiger Bereiche*. Mit dieser Aufgabe können Sie Untersuchung kritischer Bereiche des Betriebssystems auf Befehl ausführen und Einstellungen für die Untersuchung definieren.

- *Benutzerdefinierte Untersuchung von Dateien*. Mit dieser Aufgabe können Sie Einstellungen konfigurieren und speichern, die während der Untersuchung bestimmter Dateien und Verzeichnisse mit dem Befehl `kesl-control --scan-file` verwendet werden. Als Ergebnis der Ausführung des Befehls erstellt und startet die App eine temporäre Aufgabe zur Untersuchung von Dateien.

- *Untersuchung von Containern*. Mit dieser Aufgabe können Sie Untersuchung von Container und Images auf Befehl ausführen und Einstellungen für die Untersuchung definieren.

- *Benutzerdefinierte Untersuchung von Containern*. Mit dieser Aufgabe können Sie Einstellungen konfigurieren und speichern, die während der Untersuchung bestimmter Container und Images mit dem Befehl `kesl-control [-T] --scan-container` verwendet werden. Als Ergebnis der Ausführung des Befehls erstellt und startet die App eine temporäre Aufgabe zur Untersuchung von Containern.

- *Untersuchung von Wechseldatenträgern*. Mit dieser Aufgabe können Sie die Verbindung von Wechseldatenträgern mit dem Gerät in Echtzeit überwachen und die Einstellungen für die Untersuchung von Wechseldatenträgern und ihren Bootsektoren auf Schadsoftware definieren.

- *Schutz vor Web-Bedrohungen*. Mit dieser Aufgabe können Sie den Schutz vor Web-Bedrohungen aktivieren und deaktivieren und Einstellungen für die Ausführung der Komponente "Schutz vor Web-Bedrohungen" definieren.

- *Schutz vor Netzwerkbedrohungen*. Mit dieser Aufgabe können Sie den Schutz vor Netzwerkbedrohungen aktivieren und deaktivieren und Einstellungen für die Ausführung der Komponente "Schutz vor Netzwerkbedrohungen" definieren.

- *Schutz vor Verschlüsselung*. Mit dieser Aufgabe können Sie den Schutz von Dateien vor bösartiger Remote-Verschlüsselung aktivieren und deaktivieren und Einstellungen für die Komponente "Schutz vor Verschlüsselung" definieren.

- *Firewall-Verwaltung*. Mit dieser Aufgabe können Sie die Firewall-Verwaltung aktivieren und deaktivieren und Einstellungen für die Überwachung von Netzwerkverbindungen auf dem Gerät definieren.

- *Programmkontrolle*. Mit dieser Aufgabe können Sie die Programmkontrolle aktivieren und deaktivieren und Einstellungen für die Komponente "Programmkontrolle" definieren.

- *Inventarisierung*. Mit dieser Aufgabe können Sie Informationen über alle Anwendung -Dateien abrufen, die auf dem Gerät gespeichert sind.

- *Gerätekontrolle*. Mit dieser Aufgabe können Sie die Gerätekontrolle aktivieren und deaktivieren und Einstellungen für die Komponente "Gerätekontrolle" definieren. Die Aufgabe startet automatisch, wenn Kaspersky Endpoint Security gestartet wird.

- *Web-Kontrolle*. Mit dieser Aufgabe können Sie die Web-Kontrolle aktivieren und deaktivieren und Einstellungen für die Komponente "Web-Kontrolle" definieren.

- *Verhaltensanalyse*. Mit dieser Aufgabe können Sie schädliche Aktivitäten von Anwendungen im Betriebssystem überwachen. Die Aufgabe startet automatisch, wenn Kaspersky Endpoint Security gestartet wird.

- *Überwachung der Systemintegrität*. Mit dieser Aufgabe können Sie in Echtzeit Aktionen überwachen, die mit Objekten aus dem Überwachungsbereich ausgeführt werden, der in den Einstellungen der Komponente "Überwachung der Systemintegrität" angegeben ist.

- *Überwachung der System-Integrität*. Mit dieser Aufgabe können Sie Dateien und Verzeichnisse, die Sie in den Überwachungsbereich aufgenommen haben, auf Änderungen überprüfen, indem Sie den aktuellen Status des überwachten Objekts mit einem zuvor erfassten Status vergleichen.

- *Lizenzverwaltung*. Mit dieser Aufgabe können Sie eine auf dem Gerät installierte Anwendung aktivieren. Die Aufgabe startet automatisch beim Start der App und befindet sich dauerhaft im Arbeitsspeicher des Geräts. Die Aufgabe hat keine Einstellungen; Lizenzschlüssel werden über spezielle Verwaltungsbefehle verwaltet. Die Aufgabe kann nicht gestartet, beendet oder gelöscht werden.

- *Update*. Mit dieser Aufgabe können Sie die Aktualisierung der Datenbanken und Module der Anwendung nach Zeitplan oder bei Bedarf ausführen und Update-Einstellungen konfigurieren.

- *Rollback des Datenbanken-Updates*. Mit dieser Aufgabe können Sie ein Rollback des letzten Updates der Datenbanken und Module der Anwendung durchführen.

- *Integration mit Endpoint Detection and Response Expert (on-premise)* Mit dieser Aufgabe können Sie die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder Kaspersky Endpoint Detection and Response (KATA) aktivieren oder deaktivieren sowie die Integrationseinstellungen festlegen.

- *Integration mit Kaspersky Network Detection and Response (KATA)* Mit dieser Aufgabe können Sie die Integration mit Kaspersky Network Detection and Response (KATA) aktivieren oder deaktivieren und die Integrationseinstellungen festlegen.

- *Integration mit Sandbox*. Mit dieser Aufgabe können Sie die Integration der Komponente Sandbox aktivieren und deaktivieren sowie die Integrationseinstellungen festlegen.

- *Integration mit KUMA*. Mit dieser Aufgabe können Sie die Integration mit Kaspersky Unified Monitoring and Analysis Platform aktivieren und deaktivieren sowie die Integrationseinstellungen festlegen.

- *Ausführungsprävention für Objekte (EDR Expert (on-premise))*. Mit dieser Aufgabe können Sie die Verwendung der Regeln von Endpoint Detection and Response Expert (on-premise) zur Ausführungsprävention für Objekte aktivieren und deaktivieren sowie eine Liste dieser Regeln anzeigen.

- *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.

Jede Anwendungsaufgabe hat einen Namen, der in der Befehlszeile verwendet wird, eine ID und einen Typ (siehe Tabelle unten).

IDs sind für alle Aufgaben eindeutig, auch für Remote-Aufgaben. Die App verwendet die IDs gelöschter Aufgaben nicht noch einmal. Die Nummer der ID einer neuen Aufgabe folgt auf die Nummer der ID der zuletzt erstellten Aufgabe.

Bei Aufgabennamen wird die Groß-/Kleinschreibung nicht beachtet.

Während der 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 App 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 App festgelegt. Temporäre Aufgaben werden nach Abschluss automatisch gelöscht.

Aufgaben der App

Aufgabe	Aufgabenname in der Befehlszeile	Aufgaben-ID	Aufgabentyp
Schutz vor bedrohlichen Dateien	File_Threat_Protection	1	OAS
Schadsoftware-Untersuchung.	Scan_My_Computer	2	ODS
Schadsoftware-Untersuchung (benutzerdefiniert)	Benutzereingabe	ab 100	ODS
Benutzerdefinierte Untersuchung von Dateien	Scan_File	3	ODS
Untersuchung wichtiger Bereiche.	Critical_Areas_Scan	4	ODS
Update	Update	6	Update
Update (benutzerdefiniert)	Benutzereingabe	ab 100	Update

Aufgabe	Aufgabenname in der Befehlszeile	Aufgaben-ID	Aufgabentyp
Rollback.	Rollback	7	Rollback
Rollback des Datenbanken-Updates (benutzerdefiniert)	Benutzereingabe	ab 100	Rollback
Lizenzverwaltung	Lizenz	9	Lizenz
Überwachung der System-Integrität	System_Integrity_Monitoring	11	OAFIM
Überwachung der Systemintegrität (benutzerdefiniert)	Benutzereingabe	ab 100	ODFIM
Firewall-Verwaltung	Firewall_Management	12	Firewall
Schutz vor Verschlüsselung	Anti_Cryptor	13	AntiCryptor
Schutz vor Web-Bedrohungen	Web_Threat_Protection	14	WTP
Gerätekontrolle	Device_Control	15	DeviceControl
Untersuchung von Wechseldatenträgern	Removable_Drives_Scan	16	RDS
Schutz vor Netzwerkbedrohungen	Network_Threat_Protection	17	NTP
Container untersuchen	Container_Scan	18	ContainerScan
Untersuchung von Containern (benutzerdefiniert)	Benutzereingabe	ab 100	ContainerScan
Benutzerdefinierte Untersuchung von Containern	Custom_Container_Scan	19	ContainerScan
Verhaltensanalyse	Behavior_Detection	20	BehaviorDetection
Programmkontrolle	Application_Control	21	AppControl
Inventarisierung	Inventory_Scan	22	InventoryScan
Inventarisierung (benutzerdefiniert)	Benutzereingabe	ab 100	InventoryScan
Integration mit Endpoint Detection and Response Expert (on-premise)	KATAEDR	24	KATAEDR
Web-Kontrolle	Web_Control	26	WebControl
Integration mit Sandbox	Standalone_Sandbox	29	StandaloneSandbox
Ausführungsprävention für Objekte (EDR Expert (on-premise))	KATAEDR_Prevention	30	KATAEDRPrevention
Integration mit Kaspersky Network Detection and Response (KATA).	KATANDR	31	KATANDR
Ausführungsprävention für Objekte (EDR Optimum)	EDRO_Prevention	32	Prävention
Integration mit KUMA	KUMA	33	KUMA
Schutz vor E-Mail-Bedrohungen	Mail_Monitoring	35	MailMonitoring
Schutz vor BadUSB-Angriffen	Bad_USB	37	BadUSB

Sie können mit Aufgaben folgende Aktionen ausführen:

- Alle vordefinierten und benutzerdefinierten Aufgaben starten und beenden, unter Ausnahme der Aufgabe *License*.
- Aufgaben vom Typ *ODS*, *ODFIM* und *InventoryScan* anhalten und fortsetzen.
- Benutzeraufgaben erstellen und löschen. Abhängig vom Nutzungsmodus der Anwendung können Sie Aufgaben der folgenden Typen erstellen:
  - Im Standard-Modus: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* und *InventoryScan*.
  - Im Light Agent-Modus zum Schutz virtueller Umgebungen: *ODS*, *ODFIM*, *ContainerScan* und *InventoryScan*.

- Die Einstellungen aller Benutzeraufgaben und aller vordefinierten Aufgaben ändern, mit Ausnahme der Aufgaben vom Typ *Rollback* und *License*.

  Wenn die Anwendung im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, können die Einstellungen der vordefinierten Aufgabe *Update* ebenfalls nicht geändert werden.

- Den Zeitplan für den Aufgabenstart konfigurieren.

Aufgabenliste über die Befehlszeile anzeigen

Um eine Liste mit den Aufgaben der Anwendung anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-task-list [--json]
```

wobei:

`--json` – Ausgabeformat für die Liste der Anwendungsaufgaben. Wenn Sie kein Format angeben, erfolgt die Ausgabe im INI-Format.

Zeigt eine Liste mit den Aufgaben von Kaspersky Endpoint Security an.

Für jede Aufgabe werden folgende Informationen angezeigt:

- `Name` – Aufgabenname.
- `ID` – Aufgaben-ID.
- `Type` – Aufgabentyp.
- `State` – Aktueller Status der Aufgabe.

Wenn die Kaspersky Security Center-Richtlinie den Benutzern das Anzeigen und Ändern lokaler Aufgaben verbietet, sind Informationen über die Aufgaben Scan_My_Computer, Critical_Areas_Scan, Container_Scan, Inventory_Scan, Update (im Standardmodus) und Rollback (im Standardmodus) nicht verfügbar.

Aufgabenstatus über die Befehlszeile anzeigen

Führen Sie folgenden Befehl aus, um einen Aufgabenstatus anzuzeigen:

```
kesl-control --get-task-state <ID/Name der Aufgabe> [--json]
```

wobei:

- `< ID/Name der Aufgabe >` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--json` – Gibt die Einstellungen im JSON-Format aus.

Für die Aufgaben der Anwendung sind folgende grundlegende Statusvarianten vorgesehen:

- `Started` – Aufgabe wird ausgeführt
- `Starting` – Aufgabe wird gestartet
- `Stopped` – Aufgabe wurde gestoppt
- `Stopping` – Aufgabe wird gestoppt

Die Aufgaben vom Typ *ODS*, *ODFIM* und *InventoryScan* können außerdem die folgenden Statusvarianten aufweisen:

- `Pausing` – Aufgabe wird angehalten
- `Suspended` – Aufgabe wurde angehalten
- `Resuming` – Aufgabe wird fortgesetzt

Aufgabe über die Befehlszeile erstellen

Wenn die Anwendung im Standard-Modus verwendet wird, können Sie Aufgaben der folgenden Typen erstellen: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* und *InventoryScan*.

Wenn die Anwendung im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, können Sie Aufgaben der folgenden Typen erstellen: *ODS*, *ODFIM*, *ContainerScan* und *InventoryScan*.

Sie können Aufgaben mit Standardeinstellungen oder mit Einstellungen erstellen, die in einer Konfigurationsdatei angegeben sind.

Um eine Aufgabe mit Standardeinstellungen zu erstellen, führen Sie den folgenden Befehl aus:

```
kesl-control --create-task < Aufgabenname > --type < Aufgabentyp >
```

wobei:

- `< Aufgabenname >` – Name, den Sie für eine neue Aufgabe vergeben.
- `< Aufgabentyp >` ist die Bezeichnung für den Typ der Aufgabe, die Sie erstellen.

Um eine Aufgabe mit den Einstellungen zu erstellen, die in einer Konfigurationsdatei angegeben sind, führen Sie den folgenden Befehl aus:

```
kesl-control --create-task < Aufgabenname > --type < Aufgabentyp > --file < Pfad der
Konfigurationsdatei > [--json]
```

wobei:

- `< Aufgabenname >` – Name, den Sie für eine neue Aufgabe vergeben.
- `< Aufgabentyp >` ist die Kennung für den Typ der Aufgabe, die Sie erstellen.
- `< Dateipfad >` – Vollständiger Pfad der Konfigurationsdatei, deren Einstellungen beim 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.

Aufgabe über die Befehlszeile starten, beenden, anhalten und fortsetzen

Sie können vordefinierte und benutzerdefinierte Aufgaben starten und beenden, unter Ausnahme der Aufgabe License.

Sie können ODS-, ODFIM- und InventoryScan-Aufgaben anhalten und fortsetzen.

Aufgabe starten

```
kesl-control --start-task <ID|Name der Aufgabe> [-W] [--progress]
```

wobei:

- `<ID|Name der Aufgabe>` 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.

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.

Aufgabe beenden

```
kesl-control --stop-task <ID|Name der Aufgabe> [-W]
```

wobei:

- `<ID|Name der Aufgabe>` 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.

Aufgabe anhalten

```
kesl-control --suspend-task <ID|Name der Aufgabe>
```

Aufgabe fortsetzen

```
kesl-control --resume-task <ID|Name der Aufgabe>
```

Aufgabe über die Befehlszeile löschen

Sie können nur Benutzeraufgaben löschen. Vordefinierte Aufgaben können nicht gelöscht werden.

Um eine Aufgabe zu löschen, führen Sie folgenden Befehl aus:

```
kesl-control --delete-task <ID/Name der Aufgabe>
```

Wobei gilt: `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Aufgabeneinstellungen über die Befehlszeile ausgeben

Sie können die aktuellen Werte der Einstellungen aller Benutzeraufgaben und aller vordefinierten Aufgaben anzeigen, mit Ausnahme der Aufgaben *Rollback* und *License* (diese Aufgaben haben keine Einstellungen).

Sie können die aktuellen Werte von Aufgabeneinstellungen in die Konsole oder in eine Konfigurationsdatei ausgeben, die Sie verwenden können, um Aufgabeneinstellungen zu ändern.

Um die aktuellen Werte der Aufgabeneinstellungen in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings <ID/Name der Aufgabe> [--json]
```

wobei:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--json` wird 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 Aufgabeneinstellungen in eine Konfigurationsdatei auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings <ID/Name der Aufgabe> --file <Pfad der
Konfigurationsdatei> [--json]
```

wobei:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--file <Pfad der Konfigurationsdatei>` ist der Pfad zur Konfigurationsdatei, in die die Aufgabeneinstellungen geschrieben werden. Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.
- `--json` wird angegeben, um die Einstellungen im JSON-Format auszugeben. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Aufgabeneinstellungen über die Befehlszeile bearbeiten

Sie können die Einstellungen aller Benutzeraufgaben und aller vordefinierten Aufgaben ändern, mit Ausnahme der Aufgaben *Rollback* und *License*.

> Wenn die Anwendung im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, können die Einstellungen der vordefinierten Aufgabe *Update* ebenfalls nicht geändert werden.

Über die Befehlszeile können Sie die Aufgabeneinstellungen mit dem Befehl `kesl-control --set-settings` ändern:

- Sie können alle Aufgabeneinstellungen ändern, indem Sie die Konfigurationsdatei verwenden, welche die Aufgabeneinstellungen enthält. Sie können die Konfigurationsdatei mit dem Befehl zur Ausgabe der Aufgabeneinstellungen abrufen.
- Sie können einzelne Aufgabeneinstellungen bearbeiten, indem Sie Befehlszeilenoptionen im Format `<Einstellungsname>=<Einstellungswert>` verwenden. Sie können die aktuellen Werte der Aufgabeneinstellungen mit dem Befehl zur Ausgabe der Aufgabeneinstellungen abrufen.
- Sie können die Standardaufgabeneinstellungen wiederherstellen.

Sie können Untersuchungsbereiche und Ausschlussbereiche mithilfe einer Konfigurationsdatei, die Aufgabeneinstellungen oder Befehlszeilenschalter enthält, hinzufügen und entfernen. Die Konfiguration von Untersuchungsbereichen und Ausschlussbereichen ist für Aufgaben vom Typ *OAS*, *ODS*, *OAFIM*, *ODFIM* und *AntiCryptor* verfügbar.

> Bei Systemen mit dem Dateisystem BTRFS und aktivierten aktiven Snapshots wird es zur Optimierung der Untersuchungsaufgaben empfohlen, den Pfad mit dem im "Read only"-Modus gemounteten Snapshots den Ausschlüssen hinzuzufügen. Beispielsweise können in Systemen auf Basis von SUSE/OpenSUSE den Pfad für die Ausschlüsse folgendermaßen angeben: `/.snapshots/*/snapshot/`.

Einige Aufgaben verfügen auch über separate Verwaltungsbefehle, mit denen Sie Aufgabeneinstellungen ändern können.

Aufgabeneinstellungen mithilfe einer Konfigurationsdatei bearbeiten

So ändern Sie die Werte der Aufgabeneinstellungen mithilfe einer Konfigurationsdatei:

1. Geben Sie die Aufgabeneinstellungen mithilfe des Befehls `kesl-control --get-schedule` in der Konfigurationsdatei aus.

2. Öffnen Sie die Konfigurationsdatei und ändern Sie die Werte der erforderlichen Einstellungen.

   Für 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` – Pfad zum Verzeichnis mit untersuchten Objekten. Sie können den Pfad zu einem lokalen Verzeichnis angeben oder die Untersuchung von Remote-Verzeichnissen aktivieren, die auf dem Client-Gerät eingebunden sind.
   - `AreaMask.item_#` – Einschränkung des Untersuchungsbereichs. Sie können eine Maske für die Namen der zu scannenden Dateien festlegen. Standardmäßig ist die Untersuchung für alle Objekte im Untersuchungsbereich aktiviert. Sie können mehrere Elemente vom Typ `AreaMask.item_#` angeben.

   Wenn Sie einen Ausschlussbereich hinzufügen möchten, fügen Sie der Datei den Abschnitt `[ExcludedFromScanScope.item_#]` mit den folgenden Parametern hinzu:

   - `AreaDesc` – Beschreibung des Ausschlussbereichs, die zusätzliche Informationen zum Ausschlussbereich enthält.
   - `UseScanArea` – Aktiviert den Ausschluss des angegebenen Bereichs.
   - `Path` – Pfad zum Verzeichnis mit ausgeschlossenen Objekten. Sie können den Pfad zu einem lokalen Verzeichnis angeben oder Remote-Verzeichnisse ausschließen, die auf dem Client-Gerät eingebunden sind. Mögliche Einstellungswerte hängen vom Aufgabentyp ab.
   - `AreaMask.item_#` – Einschränkung des Ausschlussbereichs. Sie können eine Maske für Namen von Dateien angeben, die Sie aus dem Untersuchungsbereich ausschließen möchten. Standardmäßig sind alle Bereichsobjekte ausgeschlossen.

     Beispiel:
     ```
     [ExcludedFromScanScope.item_0000]
     AreaDesc=
     UseScanArea=Yes
     Path=/tmp/notchecked
     AreaMask.item_0000=*
     ```

   Sie können mehrere Abschnitte vom Typ `[ScanScope.item_#]` und `[ExcludedFromScanScope.item_#]` angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge.

3. Speichern Sie die Konfigurationsdatei.

4. Führen Sie den Befehl aus:

   `kesl-control --set-settings <ID/Name der Aufgabe> --file <Pfad der Konfigurationsdatei> [--json]`

   wobei:

   - `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
   - `--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die Einstellungen der Aufgabe importiert werden.
   - Geben Sie die Option `--json` an, wenn Sie Einstellungen aus einer JSON-Konfigurationsdatei 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.

Aufgabeneinstellungen mithilfe der Befehlszeilenschalter bearbeiten

Mit den Optionen des Befehls `kesl-control --set-settings` können Sie einzelne Werte der Aufgabeneinstellungen ändern sowie Untersuchungsbereiche und Ausschlussbereiche für Aufgaben der Typen *OAS*, *ODS*, *OAFIM*, *ODFIM* und *AntiCryptor* hinzufügen oder entfernen.

Einzelne Aufgabeneinstellungen konfigurieren

Um einzelne Werte der Aufgabeneinstellungen mithilfe von Befehlszeilenschaltern zu ändern, führen Sie den folgenden Befehl aus:

`kesl-control --set-settings <ID/Name der Aufgabe> <Name der Einstellung>=<Wert der Einstellung> [<Name der Einstellung>=<Wert der Einstellung>]`

wobei:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `<Name der Einstellung>=<Wert der Einstellung>` – Name und Wert einer der Aufgabeneinstellungen. Sie können die aktuellen Werte der Aufgabeneinstellungen mit dem Befehl zur Ausgabe der Aufgabeneinstellungen abrufen.

Die Werte der angegebenen Aufgabeneinstellungen werden geändert.

Wenn Sie in den Einstellungen der Aufgabe 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.

Einen Untersuchungsbereich hinzufügen oder entfernen

Um einen Untersuchungsbereich mithilfe von Befehlszeilenschaltern hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings <ID/Name der Aufgabe> --add-path <Pfad>
```

wobei:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--add-path <Pfad>` fügt einen Pfad zu einem Verzeichnis mit zu untersuchenden Objekten hinzu.

Den Aufgabeneinstellungen wird ein neuer Abschnitt vom Typ `[ScanScope.item_#]` hinzugefügt. Die Anwendung untersucht die Objekte im Verzeichnis, das im Parameter `Path` angegeben ist. Die übrigen Einstellungen für den Untersuchungsbereich nehmen Standardwerte an.

Wenn die Aufgabeneinstellungen bereits einen Abschnitt `[ScanScope.item_#]` mit dem angegebenen Wert für die Einstellung `Path` enthalten, wird kein doppelter Abschnitt hinzugefügt.

Wenn die Einstellung `UseScanArea` der Wert `No` besaß, ändert sich der Wert nach der Ausführung dieses Befehls zu `Yes` und die Objekte, die sich in diesem Verzeichnis befinden, werden untersucht.

Beispiel:
Hinzufügen eines Untersuchungsbereichs für eine Aufgabe mit der ID=100:

```
kesl-control --set-settings 100 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

Die folgenden Einstellungen für den Untersuchungsbereich werden der Aufgabe hinzugefügt:

```
[ScanScope.item_0001]

AreaDesc=

UseScanArea=Yes

Path=/home

AreaMask.item_0000=*
```

Um einen Untersuchungsbereich mithilfe von Befehlszeilenschaltern zu entfernen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings <ID/Name der Aufgabe> --del-path <Pfad>
```

wobei:

- `< ID/Name der Aufgabe >` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--del-path < Pfad >` entfernt einen Pfad zu einem Verzeichnis mit zu untersuchenden Objekten.

  Der Abschnitt `[ScanScope.item_#]`, der den angegebenen Pfad enthält, wird aus den Aufgabeneinstellungen entfernt. Die Anwendung untersucht keine der Objekte im angegebenen Verzeichnis.

Einen Ausschlussbereich hinzufügen oder entfernen

Um einen Ausschlussbereich mithilfe von Befehlszeilenschaltern hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings < ID/Name der Aufgabe > --add-exclusion < Pfad >
```

wobei:

- `< ID/Name der Aufgabe >` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--add-exclusion < Pfad >` fügt einen Pfad zu einem Verzeichnis mit Objekten hinzu, die Sie von der Untersuchung ausschließen möchten.

  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. Die übrigen Einstellungen für den Ausschlussbereich nehmen Standardwerte an.

  Wenn in den Aufgabeneinstellungen bereits ein Abschnitt vom Typ `[ExcludedFromScanScope.item_#]` mit dem angegebenen Einstellungswert `Pfad` existiert, wird der Abschnitt nicht dupliziert.

  Wenn die Einstellung `UseScanArea` den Wert `No` besaß, ändert sich der Wert nach der Ausführung dieses Befehls zu `Yes` und die Objekte, die sich in diesem Verzeichnis befinden, werden von der Untersuchung ausgeschlossen.

Um einen Ausschlussbereich mithilfe von Befehlszeilenschaltern zu entfernen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings < ID/Name der Aufgabe > --del-exclusion < Pfad >
```

wobei:

- `< ID/Name der Aufgabe >` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--del-exclusion < Pfad >` 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 Anwendung schließt keines der Objekte im angegebenen Verzeichnis von der Untersuchung aus.

Standardaufgabeneinstellungen über die Befehlszeile wiederherstellen

Sie können die Standardeinstellungen für alle Benutzeraufgaben und alle vordefinierten Aufgaben wiederherstellen, mit Ausnahme von Aufgaben der Typen *Rollback* und *License* (diese Aufgaben haben keine Einstellungen).

Um die Standardaufgabeneinstellungen über die Befehlszeile wiederherzustellen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings <ID/Name der Aufgabe> --set-to-default
```

Wobei gilt: `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Die Anwendung setzt die Werte der Einstellungen auf die Standardwerte zurück.

Aufgabenzeitplan über die Befehlszeile anpassen

Wenn die Anwendung im Standard-Modus verwendet wird, können Sie einen Zeitplan für den Start von Aufgaben der folgenden Typen erstellen: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* und *InventoryScan*.

Wenn die Anwendung im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, können Sie einen Zeitplan für den Start von Aufgaben der folgenden Typen erstellen: *ODS*, *ODFIM*, *ContainerScan* und *InventoryScan*.

Sie können die aktuellen Werte für die Einstellungen des Zeitplans für den Aufgabenstart in die Konsole oder in eine Konfigurationsdatei ausgeben.

Um die aktuellen Einstellungen des Zeitplans für den Aufgabenstart in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-schedule <ID/Name der Aufgabe> [--json]
```

wobei:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--json` wird 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 Einstellungen des Zeitplans für den Aufgabenstart in die Konfigurationsdatei auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-schedule <ID/Name der Datei> --file <Pfad der Konfigurationsdatei>
[--json]
```

wobei:

- `< ID/Name der Aufgabe >` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `--file < Pfad der Konfigurationsdatei >` ist der Pfad zur Konfigurationsdatei, in die die Einstellungen des Aufgabenzeitplans geschrieben werden. Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.
- `--json` wird angegeben, um die Einstellungen im JSON-Format auszugeben. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

  Beispiele:
  So speichern Sie die Einstellungen der Update-Aufgabe in einer neu erstellten Datei mit dem Namen update_schedule.ini im aktuellen Verzeichnis:

  ```
  kesl-control --get-schedule 6 --file update_schedule.ini
  ```

  So geben Sie den Zeitplan der Update-Aufgabe in die Konsole aus:

  ```
  kesl-control --get-schedule 6
  ```

Sie können die Einstellungen des Zeitplans für den Aufgabenstart wie folgt ändern:

- Importieren Sie die Einstellungen aus einer Konfigurationsdatei, die alle Zeitplaneinstellungen enthält.
- Geben Sie über die Befehlszeile einzelne Einstellungen des Aufgabenzeitplans im Format `< Name der Einstellung >=< Wert der Einstellung >` an.

Gehen Sie folgendermaßen vor, um die Werte der Einstellungen des Zeitplans für den Aufgabenstart mithilfe einer Konfigurationsdatei zu ändern:

1. Geben Sie die Aufgabeneinstellungen mithilfe des Befehls `kesl-control --get-schedule` in die Konfigurationsdatei aus.
2. Ändern Sie die Werte der erforderlichen Einstellungen in der Datei und speichern Sie die Änderungen.
3. Führen Sie den Befehl aus:

   ```
   kesl-control --set-schedule < ID/Name der Datei > --file < Pfad der Konfigurationsdatei > [--json]
   ```

   wobei:

   - `< ID/Name der Aufgabe >` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
   - `--file < Pfad der Konfigurationsdatei >` – Vollständiger Pfad der Konfigurationsdatei, aus der die Einstellungen des Aufgabenzeitplans importiert werden.
   - Geben Sie die Option `--json` an, wenn Sie Einstellungen aus einer JSON-Konfigurationsdatei 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 des Zeitplans für den Aufgabenstart werden in die Anwendung importiert.

Beispiel:
Zeitplaneinstellungen aus der Konfigurationsdatei /home/test/on_demand_schedule.ini in die Aufgabe mit ID=2 importieren:

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

Um einzelne Werte der Einstellungen des Zeitplans für den Aufgabenstart mithilfe der Befehlszeile zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-schedule <ID/Name der Aufgabe> <Name der Einstellung>=<Wert der Einstellung> [<Name der Einstellung>=<Wert der Einstellung>]
```

wobei:

- `<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.
- `<Name der Einstellung>=<Wert der Einstellung>` ist der Name und der Wert einer der Einstellungen des Aufgabenzeitplans.

Die Werte der angegebenen Einstellungen des Zeitplans für den Aufgabenstart werden geändert.

Beispiele:

Geben Sie die folgenden Einstellungen an, damit die Aufgabe nach Zeitplan alle zehn Stunden gestartet wird:

```
RuleType=Hourly

RunMissedStartRules=No

StartTime=2021/May/30 23:05:00;10

RandomInterval=0
```

Geben Sie die folgenden Einstellungen an, damit die Aufgabe nach Zeitplan alle zehn Minuten gestartet wird:

```
RuleType=Minutely

RunMissedStartRules=No

StartTime=23:10:00;10

RandomInterval=0
```

Geben Sie die folgenden Einstellungen an, damit die Aufgabe nach Zeitplan am 15. jeden Monats gestartet wird:

```
RuleType=Monthly

RunMissedStartRules=No

StartTime=23:25:00;15

RandomInterval=0
```

Geben Sie die folgenden Einstellungen an, damit die Aufgabe nach Zeitplan jeden Dienstag gestartet wird:

```
RuleType=Weekly

StartTime=18:01:30;Tue

RandomInterval=99

RunMissedStartRules=No
```

Geben Sie die folgenden Einstellungen an, damit die Aufgabe nach Zeitplan alle 11 Tage gestartet wird:

```
RuleType=Daily

RunMissedStartRules=No

StartTime=23:15:00;11

RandomInterval=0
```

Allgemeine App-Einstellungen über die Befehlszeile verwalten

Die allgemeinen Anwendungseinstellungen bestimmen die Ausführung der Anwendung als Ganzes und die Ausführung einzelner Funktionen.

Sie können die allgemeinen Anwendungseinstellungen mithilfe spezieller Verwaltungsbefehle verwalten:

- Geben Sie die aktuellen Werte der allgemeinen Anwendungseinstellungen in die Konsole oder in eine Konfigurationsdatei aus.
- Bearbeiten Sie allgemeine App-Einstellungen mithilfe einer Konfigurationsdatei, die alle allgemeinen Einstellungen enthält, oder mithilfe von Befehlszeilenoptionen im Format `<Name der Einstellung>=<Wert der Einstellung>`.

Mit den allgemeinen Einstellungen können Sie Folgendes tun:

- Konfigurieren Sie die Verwendung von Kaspersky Security Network und einer schlankeren Version der Malware-Datenbanken in der Anwendung.
- 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 Ausschlüsse von der Untersuchung des Arbeitsspeichers.
- Aktivieren und deaktivieren Sie die Untersuchung von Containern 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 für Untersuchungsaufgaben (z. B. vom Typ ODS).
- Begrenzen Sie die Anzahl der benutzerdefinierten Untersuchungsaufgaben, die ein nicht privilegierter Benutzer gleichzeitig ausführen kann.

Allgemeine Anwendungseinstellungen ausgeben

Sie können die aktuellen Werte der allgemeinen Anwendungseinstellungen in die Konsole oder in eine Konfigurationsdatei ausgeben, die Sie verwenden können, um Anwendungseinstellungen zu ändern.

Um die aktuellen Werte der allgemeinen Anwendungseinstellungen in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-app-settings [--json]
```

wobei `--json` angegeben wird, 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 allgemeinen Anwendungseinstellungen in eine Konfigurationsdatei auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-app-settings --file <Pfad zur Konfigurationsdatei> [--json]
```

wobei:

- `--file <Pfad der Konfigurationsdatei>` – Pfad der Konfigurationsdatei, in der die allgemeinen Anwendungseinstellungen ausgegeben werden. Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.
- `--json` wird angegeben, um die Einstellungen im JSON-Format auszugeben. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Beispiel:
Geben Sie die allgemeinen App-Einstellungen in eine Datei mit dem Namen kesl_config.ini aus. Speichern Sie die erstellte Datei im aktuellen Verzeichnis:

```
kesl-control --get-app-settings --file kesl_config.ini
```

Allgemeine Anwendungseinstellungen ändern

Über die Befehlszeile können Sie die allgemeinen Programmeinstellungen mit dem Befehl `kesl-control --set-app-settings` ändern:

- Sie können alle allgemeinen Einstellungen ändern, indem Sie die Konfigurationsdatei verwenden, welche die allgemeinen Anwendungseinstellungen enthält. Sie können die Konfigurationsdatei mit dem Befehl zur Ausgabe der allgemeinen Einstellungen abrufen.
- Sie können einzelne Einstellungen mithilfe von Befehlszeilenoptionen im Format `<Einstellungsname>=<Einstellungswert>` bearbeiten. Sie können die aktuellen Werte der allgemeinen Einstellungen mit dem Befehl zur Ausgabe der allgemeinen Einstellungen abrufen.

So ändern Sie die Werte der allgemeinen Einstellungen mithilfe einer Konfigurationsdatei:

1. Geben Sie die allgemeinen Anwendungseinstellungen in eine Konfigurationsdatei aus.
2. Ändern Sie die Werte der erforderlichen Einstellungen in der Datei und speichern Sie die Änderungen.
3. Führen Sie den Befehl aus:

   ```
   kesl-control --set-app-settings --file <Pfad zur Konfigurationsdatei> [--json]
   ```

   wobei:

   - `--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei mit den allgemeinen Anwendungseinstellungen. Wenn Sie einen beliebigen Parameter in der Konfigurationsdatei löschen, wird nach Ausführung des Befehls der Standardwert für diesen Parameter zugewiesen.
   - Geben Sie die Option `--json` an, wenn Sie Einstellungen aus einer JSON-Konfigurationsdatei 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.

Um die Werte der allgemeinen Einstellungen mithilfe von Befehlszeilenschaltern zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-app-settings <Name der Einstellung>=<Wert der Einstellung> [<Name der Einstellung>=<Wert der Einstellung>]
```

Wobei gilt: `<Name der Einstellung>=<Wert der Einstellung>` – Name und Wert einer der allgemeinen Anwendungseinstellungen.

Die Werte der angegebenen allgemeinen Einstellungen werden geändert.

Beispiele:

Allgemeine Einstellungen aus der Konfigurationsdatei /home/test/kesl_config.ini in die Anwendung importieren:

```
kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

Niedrigen Detaillierungsgrad für die Protokolldatei festlegen:

```
kesl-control --set-app-settings TraceLevel=NotDetailed
```

Fügen Sie den Mountpunkt hinzu, den Sie vom Modul zum Abfangen von Dateioperationen ausschließen möchten:

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/data"
```

Filter zur Eingrenzung der Abfrageergebnisse verwenden

Mit einem Filter können Sie die Ergebnisse einer Abfrage beim Ausführen von Befehlen zur 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:

```
"<Feld> <Vergleichsoperator> '<Wert>'"
```

```
"<Feld> <Vergleichsoperator> '<Wert>' and <Feld> <Vergleichsoperator> '<Wert>'"
```

wobei:

- `<Feld>` ist der Name des Datenbankfelds.
- `<Vergleichsoperator>` – Einer der folgenden Vergleichsoperatoren:
  - `>` – Größer als.
  - `<` – 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.
- `<=` – Kleiner oder gleich.

- `<Wert>` – Feldwert. Der Wert muss in einfachen Anführungszeichen (') angegeben werden.

  Sie können den Datumswert als Unix™-Zeitstempel (Anzahl der vergangenen Sekunden seit 1. Januar 1970, 00:00:00 Uhr (UTC)) oder im Format 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.

Sie können den Filter in den folgenden Befehlen zur Anwendungsverwaltung verwenden:

- Informationen zu bestimmten aktuellen Programmereignissen ausgeben (Ereignisse in der Befehlszeile anzeigen, Ereignisse in Kaspersky Security Center anzeigen):

  ```
  kesl-control -W --query "<Filterbedingungen>"
  ```

- Informationen zu bestimmten Programmereignissen im Ereignisprotokoll ausgeben (Ereignisse in der Befehlszeile anzeigen, Ereignisse in Kaspersky Security Center anzeigen):

  ```
  kesl-control -E --query "<Filterbedingungen>"
  ```

- Abrufen von Informationen zu bestimmten Objekten im Backup:

  ```
  kesl-control -B --query "<Filterbedingungen>"
  ```

- Löschen bestimmter Objekte aus dem Backup:

  ```
  kesl-control -B --mass-remove --query "<Filterbedingungen>"
  ```

  Beispiele:
  Abrufen von Informationen zu Ereignissen, die den Text "etc" im Feld "FileName" enthalten:

  ```
  kesl-control -E --query "FileName like '%etc%'"
  ```

  Abrufen von Ereignissen vom Typ "ThreatDetected" (Bedrohung erkannt):

  ```
  kesl-control -E --query "EventType == 'ThreatDetected'"
  ```

  Abrufen von Informationen zu Ereignissen vom Typ "ThreatDetected", die von Aufgaben des Typs "ODS" generiert wurden:

  ```
  kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"
  ```

  Abrufen von Informationen zu Ereignissen, die nach einem bestimmten Datum generiert wurden (Angabe im Zeitformat UNIX™, d. h. der Anzahl an Sekunden, die seit 00:00:00 (UTC), 1. Januar 1970 vergangen sind):

  ```
  kesl-control -E --query "Date > '1583425000'"
  ```

  Abrufen von Informationen zu Ereignissen, die nach dem im Format "JJJJ-MM-TT hh:mm:ss" angegebenen Datum generiert wurden:

  ```
  kesl-control -E --query "Date > '2022-12-22 18:52:45'"
  ```

  Abrufen von Informationen zu Dateien im Backup mit der Signifikanz "High":

  ```
  kesl-control -B --query "DangerLevel == 'High'"
  ```

Anwendungseinstellungen exportieren und importieren

Wenn Sie Kaspersky Endpoint Security mithilfe von Kaspersky Security Center verwalten, ist der Import von Einstellungen nicht verfügbar.

Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, können die Einstellungen der vordefinierten Aufgabe vom Typ *Update* nicht exportiert oder importiert werden.

In Kaspersky Endpoint Security können zur Fehlerbehebung, Überprüfung der Einstellungen oder zur einfacheren Konfiguration der Anwendung auf Benutzergeräten alle Anwendungseinstellungen exportiert und importiert werden. 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 Einstellungen in die Anwendung zu importieren.

Während des Imports und Exports von Einstellungen muss die Anwendung ausgeführt werden. Nach dem Import der Einstellungen ist ein Neustart der Anwendung erforderlich.

Beim Importieren oder Exportieren von Einstellungen aus älteren Versionen der Anwendung, werden für neue Einstellungen die Standardwerte verwendet. Das Importieren von Einstellungen in eine ältere Version der Anwendung ist nicht möglich.

Um Anwendungseinstellungen zu exportieren, führen Sie den folgenden Befehl aus:

```
kesl-control --export-settings --file <Pfad zur Konfigurationsdatei> [--json]
```

wobei:

- `--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, in der die Anwendungseinstellungen gespeichert werden.
- `--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.

Um Anwendungseinstellungen aus einer Datei zu importieren, führen Sie den folgenden Befehl aus:

```
kesl-control --import-settings --file <Pfad zur Konfigurationsdatei> [--json]
```

wobei:

- `--file <Pfad zur Konfigurationsdatei>` ist der vollständige Pfad zur Konfigurationsdatei, aus der die Einstellungen in das Programm importiert 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.

Beim Import der Parameter aus einer Datei wird für die Parameter `UseKSN` und `CloudMode` der Wert `No` festgelegt und die Integration mit MDR deaktiviert. Um die Verwendung von Kaspersky Security Network zu beginnen oder fortzusetzen, müssen Sie für den Parameter `UseKSN` den Wert `Basic` oder `Extended` festlegen. Um den Cloud-Modus zu aktivieren, müssen Sie für den Parameter `CloudMode` den Wert `Yes` festlegen. Der Cloud-Modus ist verfügbar, wenn KSN aktiviert ist. Um die Integration mit MDR zu aktivieren, müssen Sie zunächst die Verwendung von Kaspersky Security Network im erweiterten Modus aktivieren und anschließend für den Parameter `UseMDR` den Wert `Yes` festlegen.

Durch dem Import der Anwendungseinstellungen können sich die internen Aufgaben-IDs ändern. Es wird empfohlen, zur Aufgabenverwaltung die Aufgabennamen zu verwenden.

Die folgenden Richtlinieneinstellungen können nicht aus Version 12.3 des Web-Plug-ins für das Programm in die Programmversion 12.4 importiert werden:

- 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)

Benutzerrollen über die Befehlszeile verwalten

Benutzer können entsprechend ihren Rollen über die Befehlszeile auf die Funktionen von Kaspersky Endpoint Security zugreifen. *Rolle* – Eine Reihe von Rechten und Berechtigungen zur Verwaltung der Anwendung.

Im Betriebssystem werden vier Gruppen mit Systembenutzern erstellt: *kesladmin*, *kesluser*, *keslaudit* und *nokesl*. Wenn eine Rolle der Anwendung einem Benutzer des Systems zugewiesen wird, wird der Benutzer zur entsprechenden Gruppe hinzugefügt (s. nachfolgende Tabelle *Rollen*). Sollte einem Benutzer eine Rolle entzogen werden, wird der Benutzer aus der entsprechenden Gruppe entfernt.

Wenn einem Systembenutzer keine Rolle für die Anwendung zugewiesen wurde, gehört dieser Benutzer zur entsprechenden Gruppe *Benutzer ohne Berechtigungen*.

Somit entsprechen die Rollen vier Gruppen von Benutzern des Betriebssystems:

- kesladmin entspricht der Rolle "Administrator".
- kesluser entspricht der Rolle "Benutzer".
- keslaudit entspricht der Rolle "Auditor",
- nokesl wird einem Benutzer zugewiesen, dem keine andere Rolle zugewiesen ist. In diesem Fall gehört der Benutzer zu einer spezifischen Gruppe der *Benutzer ohne Berechtigungen*.

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.

Benutzerrollen

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`. Lizenzierung der Anwendung verwalten Rollen an Benutzer zuweisen Benutzerrollen entziehen (der Administrator kann sich die Rolle "admin" nicht selbst entziehen) Speicher der Benutzer anzeigen und verwalten
Benutzer	Benutzer	kesluser	Nur Aufgaben für die benutzerdefinierte Untersuchung von Dateien verwalten Update-Aufgaben starten und beenden Berichte für von Benutzern erstellte Aufgaben anzeigen Anzeigen von Ereignissen, die für alle Benutzer der Anwendung gelten
Auditor	audit	keslaudit	Anwendungseinstellungen 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.

Liste von Benutzern und Rollen anzeigen

Um eine Liste der Benutzer und deren Rollen anzuzeigen, führen Sie folgenden Befehl aus:

```
kesl-control [-U] --get-user-list
```

Einem Benutzer eine Rolle zuweisen

Um einem bestimmten Benutzer eine Rolle zuzuweisen, führen Sie folgenden Befehl aus:

```
kesl-control [-U] --grant-role <Rolle> <Benutzer>
```

Beispiel:
So weisen Sie dem Benutzer test15 die Rolle "audit" zu:

```
kesl-control --grant-role audit test15
```

Einem Benutzer eine Rolle entziehen

Um einem bestimmten Benutzer eine Rolle zu entziehen, führen Sie folgenden Befehl aus:

```
kesl-control [-U] --revoke-role <Rolle> <Benutzer>
```

Beispiel:
So entziehen Sie dem Benutzer test15 die Rolle "audit":

```
kesl-control --revoke-role audit test15
```

Anwendung starten und beenden

Nach der Installation von Kaspersky Endpoint Security auf dem Gerät wird die Anwendung automatisch gestartet. Danach wird die Anwendung standardmäßig automatisch gestartet, wenn das Betriebssystem hochfährt (innerhalb der Standardausführungsebene für jedes Betriebssystem).

Standardmäßig werden beim Start von Kaspersky Endpoint Security automatisch die folgenden Funktionskomponenten der Anwendung gestartet:

- Schutz vor bedrohlichen Dateien.
- Gerätekontrolle.
- Verhaltensanalyse.
- Schutz vor Web-Bedrohungen – Nur wenn einer der unterstützten Browser im Betriebssystem installiert ist und die lokale Verwaltung der Einstellungen für den Schutz vor Web-Bedrohungen auf dem Gerät zugelassen ist (die Richtlinie wird nicht angewendet oder das "Schloss" ist in den Eigenschaften der Richtlinie nicht gesetzt).
- Schutz vor Netzwerkbedrohungen – Nur wenn die Einstellungen für den Schutz vor Netzwerkbedrohungen auf dem Gerät durch eine Richtlinie festgelegt werden. Standardmäßig ist in den Eigenschaften die Richtlinie der Schutz vor Netzwerkbedrohungen aktiviert. Wenn auf das Gerät lokal konfigurierte Einstellungen angewendet werden, ist der Schutz vor Netzwerkbedrohungen standardmäßig deaktiviert.

Wenn Sie die Anwendung auf dem Gerät starten, werden automatisch Dienstaufgaben gestartet, um die Ausführung zusätzlicher Anwendungsfunktionen sicherzustellen: Funktionen zur Aktivierung der Anwendung und Backup-Funktionen.

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 Anwendung beenden, werden alle momentan auf dem Gerät laufenden Aufgaben unterbrochen. Unterbrochene Benutzeraufgaben werden nach dem Neustart der Anwendung nicht automatisch fortgesetzt.

Anwendung mithilfe von Web Console starten und beenden

So starten oder beenden Sie die Anwendung aus der Ferne:

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

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie in der Liste das Gerät aus, auf dem Sie die 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.

Anwendung mithilfe der Verwaltungskonsole starten und beenden

So starten oder beenden Sie die Anwendung auf einem Client-Gerät:

1. Wählen Sie in der Struktur der Verwaltungskonsole im Ordner **Verwaltete Geräte** die Administrationsgruppe aus, die das benötigte Gerät enthält.
2. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.
3. Wählen Sie in der Liste der verwalteten Geräte das Gerät aus, auf dem Sie die App starten oder stoppen möchten. 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:

   - Wenn Sie die Anwendung ausführen möchten, klicken Sie auf die Schaltfläche rechts neben der Liste der Kaspersky-Anwendungen oder wählen Sie im Kontextmenü der Anwendung den Punkt **Starten**.
   - Wenn Sie die Anwendung beenden möchten, klicken Sie auf die Schaltfläche rechts neben der Liste der Kaspersky-Anwendungen oder wählen Sie im Kontextmenü der Anwendung den Punkt **Stoppen**.

App über die Befehlszeile starten und beenden

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.

Kaspersky Endpoint Security starten, neu starten und beenden

Um die Anwendung zu starten, führen Sie folgenden Befehl aus:

```
systemctl start kesl
```

Um die Anwendung zu stoppen, führen Sie folgenden Befehl aus:

```
systemctl stop kesl
```

Um die Anwendung erneut zu starten, führen Sie folgenden Befehl aus:

```
systemctl restart kesl
```

Überwachen des Status 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.

Um den Anwendungsstatus auszugeben, führen Sie den folgenden Befehl aus:

```
systemctl status kesl
```

Informationen zum Schutzstatus des Geräts und zur Programmleistung anzeigen

Sie können Informationen zum Schutzstatus des Geräts und zum Ausführungsstatus von Kaspersky Endpoint Security und seiner Komponenten auf dem Gerät anzeigen.

Sie können Informationen über den Schutzstatus des Geräts auf folgende Arten abrufen:

- In der Web Console oder in der Verwaltungskonsole mithilfe der Status der Client-Geräte (*OK*, *Kritisch*, *Warnung*). Das Gerät, auf dem der Kaspersky Security Center Administrationsagent installiert ist, ist ein Client-Gerät für Kaspersky Security Center. Der Status eines Client-Geräts kann sich aus folgenden Gründen in *Kritisch* oder *Warnung* ändern:

  - Gemäß den in Kaspersky Security Center definierten Regeln. Der Status ändert sich beispielsweise, wenn auf dem Gerät keine Schutz-Anwendung installiert ist, eine Virenprüfung längere Zeit nicht durchgeführt wurde, die Anwendungsdatenbanken veraltet sind, die Lizenz abgelaufen ist oder die Anwendung nicht stabil ausgeführt wird. Weitere Informationen zu den Gründen für Statusänderungen und zum Festlegen der Bedingungen für die Zuweisung von Status finden Sie in der Hilfe zu Kaspersky Security Center.

  - Kaspersky Security Center empfängt den Gerätestatus von der verwalteten Anwendung, also von Kaspersky Endpoint Security.

    Der Empfang eines Gerätestatus von einer verwalteten Anwendung muss in Kaspersky Security Center in den Listen der Bedingungen für die Zuweisung der Status *Kritisch* und *Warnung* aktiviert sein. Die Bedingungen für die Zuweisung von Gerätestatus werden im Eigenschaftenfenster der Administrationsgruppe konfiguriert.

  Weitere Informationen zu den Status von Client-Geräten finden Sie in der Hilfe zu Kaspersky Security Center.

- In der Web Console oder in der Verwaltungskonsole mithilfe der Status der Funktionskomponenten von Kaspersky Endpoint Security auf dem Gerät. In den Eigenschaften der auf dem Gerät installierten Anwendung Kaspersky Endpoint Security wird eine Liste der Funktionskomponenten der Anwendung angezeigt. Für jede Komponente wird ihr Status angezeigt.

- Über die Befehlszeile mithilfe der folgenden Verwaltungsbefehle der Anwendung:

  - Befehl `kesl-control --app-info`, welcher Informationen über die Ausführung der Anwendung und den Status der Funktionskomponenten und Aufgaben der Anwendung anzeigt.

  - Der Befehl `kesl-control --supported-tech-info`, der eine Liste der Programmfunktionen, Informationen über deren Status (verwendet oder nicht verwendet) und die Linux-Technologien anzeigt, mit denen diese Programmfunktionen implementiert sind.

  - Befehl `kesl-control --get-statistic`, welcher eine Statistik zur Anwendungsausführung und eine Liste der Mount-Punkte ausgibt.

  - Befehl `kesl-control --export-metrics`, welcher Metriken zum Zustand des Betriebssystems ausgibt.

Schutzstatus des Geräts in der Web Console anzeigen

So zeigen Sie den Schutzstatus des Geräts in der Web Console an:

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

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** oberhalb der Liste der verwalteten Geräte und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

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

3. Suchen Sie in der Liste das Gerät, für das Sie Informationen anzeigen möchten, und klicken Sie auf den Gerätenamen.

4. Wählen Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts auf der Registerkarte **Allgemein** den Abschnitt **Schutz** aus.

Im Abschnitt **Schutz** werden folgende Informationen über das Gerät angezeigt:

- **Sichtbar im Netzwerk** – Sichtbarkeit des ausgewählten Geräts im Netzwerk: *Ja* oder *Nein*.
- **Gerätestatus** – Status des Client-Geräts, der auf der Grundlage der vom Administrator festgelegten Kriterien für den Schutzstatus auf dem ausgewählten Gerät und die Aktivität des Geräts im Netzwerk generiert wird: *OK*, *Kritisch* oder *Warnung*.
- **Statusbeschreibung** – Ursachen für die Änderung des Gerätestatus zu *Kritisch* oder *Warnung*.
- **Schutzstatus** – Aktueller Status des Schutzes vor bedrohlichen Dateien auf dem ausgewählten Gerät, z. B.: *Wird ausgeführt*, *Beendet*, *Angehalten*.
- **Letzte vollständige Untersuchung** – Datum und Uhrzeit der letzten Durchführung einer vollständigen Untersuchung auf dem ausgewählten Gerät.
- **Virus gefunden** – Gesamtmenge der bösartigen Objekte, die seit dem Installationsdatum der Anwendung Kaspersky Endpoint Security auf dem ausgewählten Gerät gefunden wurden (Zähler der gefundenen Bedrohungen).
- **Objekte, die nicht desinfiziert werden konnten** – Anzahl der infizierten Objekte, die von der Anwendung Kaspersky Endpoint Security nicht desinfiziert werden konnten.

Schutzstatus des Geräts in der Verwaltungskonsole anzeigen

So zeigen Sie den Schutzstatus des Geräts in der Verwaltungskonsole an:

1. Wählen Sie in der Struktur der Verwaltungskonsole im Ordner **Verwaltete Geräte** die Administrationsgruppe aus, die das benötigte Gerät enthält.

2. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.

3. Wählen Sie in der Liste der verwalteten Geräte das erforderliche Gerät aus und öffnen Sie das Fenster **Eigenschaften: <Gerätename>** mit einem Doppelklick.

4. Wählen Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts den Abschnitt **Schutz** aus.

Im Abschnitt **Schutz** werden folgende Informationen über das Gerät angezeigt:

- **Gerätestatus** – Status des Client-Geräts, der auf der Grundlage der vom Administrator festgelegten Kriterien für den Schutzstatus auf dem Gerät und die Aktivität des Geräts im Netzwerk generiert wird.

- **Alle Probleme** – Vollständige Liste der Probleme, die von den verwalteten 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.

Informationen über die Ausführung der Anwendung in der Web Console anzeigen

So zeigen Sie Informationen über die Ausführung der Anwendung in der Web Console an:

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

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** oberhalb der Liste der verwalteten Geräte und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

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

3. Suchen Sie in der Liste das Gerät, für das Sie Informationen anzeigen möchten, und klicken Sie auf den Gerätenamen.

4. 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.

In dem Fenster werden die folgenden Informationen über die Anwendung "Kaspersky Endpoint Security" angezeigt:

- Die Registerkarte **Allgemein** im Abschnitt **Informationen** enthält allgemeine Informationen zur installierten Anwendung:
  - **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.
  - **Aktueller Status** – Status des Schutzes vor bedrohlichen Dateien, z. B.: *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.
- Die Registerkarte **Allgemein** im Abschnitt **Lizenzen** enthält Informationen über die der Anwendung hinzugefügten Lizenzschlüssel und über die mit diesen Schlüsseln verknüpften Lizenzen.
- Die Registerkarte **Allgemein** im Abschnitt **Komponenten** enthält eine Liste der funktionalen Komponenten der Anwendung. Für jede Komponente wird ihr Status (z. B. *Gestoppt, Angehalten, Nicht installiert*) und ihre Version angezeigt.

  In der Zeile **Light Agent-Modus zum Schutz virtueller Umgebungen** können Sie Informationen über die Art der Verwendung der Anwendung anzeigen:
  - Der *Ausführungsstatus* gibt an, dass die Anwendung im Light Agent-Modus verwendet wird.
  - Der Status *Nicht installiert* bedeutet, dass das Programm im Standard-Modus verwendet wird.
- Auf der Registerkarte **Ereignisse** wird eine Liste mit den Ereignissen der Anwendung auf dem Gerät angezeigt.

- Die Registerkarte **Ereigniskonfiguration** zeigt die Arten der Ereignisse, welche die App im Ereignisspeicher speichert, sowie deren Speicherdauer an.
- Auf der Registerkarte **Anwendungseinstellungen** können Sie Folgendes tun:
  - Im Abschnitt **Detection and Response** können Sie die Netzwerkisolation des Geräts verwalten.
  - Im Abschnitt **Programmkontrolle** können Sie die konfigurierten Einstellungen einer Komponente oder Programmkategorie in eine Datei exportieren und aus einer Datei importieren.
  - Im Abschnitt **Statistik** können Sie Ausführungsstatistiken der Anwendung sowie eine Liste mit Mountpunkten anzeigen.

Informationen über die Ausführung der Anwendung in der Verwaltungskonsole anzeigen

So zeigen Sie Informationen über die Ausführung der Anwendung in der Verwaltungskonsole von Kaspersky Security Center an:

1. Wählen Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center im Ordner **Verwaltete Geräte** die Administrationsgruppe aus, die das benötigte Gerät enthält.
2. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.
3. Wählen Sie in der Liste der verwalteten Geräte das erforderliche Gerät aus und öffnen Sie das Fenster **Eigenschaften: <Gerätename>** mit einem Doppelklick.
4. Wählen Sie im angezeigten Eigenschaftenfenster des verwalteten Geräts den Abschnitt **Anwendungen** aus.

   Im rechten Teil des Fensters wird eine Liste der auf dem Gerät installierten 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.

In dem Fenster werden die folgenden Informationen über die Anwendung "Kaspersky Endpoint Security" angezeigt:

- Im Abschnitt **Allgemein** finden Sie allgemeine Informationen zur installierten Anwendung:
  - **Versionsnummer**: die Versionsnummer des Programms.
  - **Installiert** – Datum und Uhrzeit der Installation der Anwendung auf dem Gerät.
  - **Aktueller Status** – Status des Schutzes vor bedrohlichen Dateien, z. B.: *Wird ausgeführt* oder *Angehalten*.
  - **Letztes Software-Update**: Datum und Uhrzeit des letzten Updates der 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.

- Im Abschnitt **Programmkontrolle** können Sie die konfigurierten Einstellungen einer Komponente oder Programmkategorie in eine Datei exportieren und aus einer Datei importieren.
- Im Abschnitt **Statistik** werden die Ausführungsstatistiken der Anwendung sowie Informationen zu den Mountpunkten angezeigt.
- Der Abschnitt **Komponenten** enthält eine Liste der Standardkomponenten der Anwendung. Für jede Komponente wird ihr Status (z. B. *Gestoppt, Angehalten, Nicht installiert*) und ihre Version angezeigt.

  In der Zeile **Light Agent-Modus zum Schutz virtueller Umgebungen** können Sie Informationen über die Art der Verwendung der Anwendung anzeigen:

  - Der *Ausführungsstatus* gibt an, dass die Anwendung im Light Agent-Modus verwendet wird.
  - Der Status *Nicht installiert* bedeutet, dass das Programm im Standard-Modus verwendet wird.
- Der Abschnitt **Lizenzschlüssel** enthält Informationen zum aktiven Lizenzschlüssel und zum Reserve-Lizenzschlüssel:
- Der Abschnitt **Ereigniskonfiguration** zeigt die Arten der Ereignisse, welche die Anwendung im Ereignisspeicher speichert, sowie deren Speicherdauer an.
- Der Abschnitt **Erweitert** enthält Informationen zum Verwaltungs-Plug-in für die App.

Informationen über die Ausführung der Anwendung über die Befehlszeile anzeigen

Um Informationen zur Anwendung anzuzeigen, führen Sie diesen Befehl aus:

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

Wobei gilt: `--json` – Gibt Daten im JSON-Format aus. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

- **Name**. Anwendungsname.
- **Version**. Aktuelle Version der Anwendung.
- **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 über die Parameter des Administrationsagenten finden Sie in der Hilfe zu Kaspersky Security Center.

- Informationen über die Hauptlizenz, unter der die Anwendung verwendet wird:
  - **Lizenzinformationen des Programms** Lizenzinformationen des Programms oder Status des Lizenzschlüssels des Programms.
  - **Ablaufdatum der Lizenz für Kaspersky Endpoint Security**. Datum und Uhrzeit (UTC) des Ablaufs der Gültigkeit der Lizenz der Anwendung.
- Informationen über die Lizenz zur Aktivierung zusätzlicher Funktionen der Anwendung. Die Felder werden angezeigt, wenn dem geschützten Gerät Schlüssel für zusätzliche Funktionen hinzugefügt wurden:
  - **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.
  - **Information über die Lizenz von EDR Expert (on-premise)**. Informationen über die Lizenz, unter der Kaspersky Endpoint Detection and Response Expert (on-premise) aktiviert wurde, oder über den Status des Lizenzschlüssels von EDR Expert (on-premise).
  - **Ablaufdatum der Lizenz von EDR Expert (on-premise)**. Datum und Uhrzeit (UTC) des Ablaufs der Gültigkeit der Lizenz.
- **Abonnementstatus**. Status des Abonnements. Dieses Feld wird angezeigt, wenn die Anwendung 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.
- Status des **Backup-Speichers**. Informationen zum Status des Backup-Speichers.

- **Verwendung des Backup-Speichers**. 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.
- **Geladene Anwendungsdatenbanken**. Informationen darüber, ob die Anwendungsdatenbanken 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 zum Schutz virtueller Umgebungen**. Informationen über die Verwendung des Programms im Light Agent-Modus zum Schutz virtueller Umgebungen. 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 darüber, dass die Anwendung im Modus als Endpoint Detection and Response Agent verwendet wird. 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: `Aktiviert`, `Deaktiviert`.
- **Integration mit Kaspersky Endpoint Detection and Response Optimum** Status der Integration mit Kaspersky Endpoint Detection and Response Optimum.
- **Schutz vor bedrohlichen Dateien**. Status des Schutzes vor bedrohlichen Dateien in Echtzeit.
- **Container-Überwachung**. Status der Echtzeit-Untersuchung von Containern (Untersuchung von Containern, Container-Überwachung).
- **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 mit Endpoint Detection and Response Expert (on-premise)** Status der Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA).
- **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 Updates der Anwendung und Aktionen, die der Benutzer ausführen muss.
- **Anwendungsausführung ist instabil**. Zeigt Informationen zum Absturz der Anwendung und zum Erstellen einer Dump-Datei an. Dieses Feld wird angezeigt, wenn es beim vorherigen Start der Anwendung einen Absturz gab.

Statistiken zur Ausführung der Anwendung anzeigen

Um die Leistung zu verbessern, können Sie zu den Untersuchungsausschlüssen folgenden Objekte hinzufügen: Dateien, die am häufigsten von der Komponente Schutz vor bedrohlichen Dateien untersucht werden; Pfade der Prozesse, die von der Komponente Verhaltensanalyse am häufigsten untersucht werden; Mountpunkte, die auf dem Gerät erkannt wurden.

> Auf Geräten mit Betriebssystemen, von denen die fanotify-Technologie unterstützt wird, stellt das Hinzufügen der Mountpunkte zu den Ausnahmen die wirksamste Möglichkeit zur Leistungssteigerung dar.

Sie können die Statistiken zu den am häufigsten untersuchten Dateien und gestarteten Prozesse sowie der Liste mit erkannten Mountpunkten auf folgende Weise anzeigen:

- in der Web Console
- in der Verwaltungskonsole
- über die Befehlszeile

Die Parameter für die Berechnung und Anzeige der Anwendungsstatistiken können Sie in der Konfigurationsdatei kesl.ini im Abschnitt `[ScannerImpactStats]` konfigurieren.

Statistiken zur Ausführung der Anwendung in der Web Console anzeigen

So zeigen Sie die Statistiken zur Ausführung der Anwendung in der Web Console an:

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

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** oberhalb der Liste der verwalteten Geräte und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

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

3. Suchen Sie in der Liste das Gerät, für das Sie Informationen anzeigen möchten, und klicken Sie auf den Gerätenamen.

4. 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.

   Das Fenster **Untersuchungsstatistiken** wird geöffnet.

   Im Fenster **Untersuchungsstatistiken** werden die folgenden Ausführungsstatistiken der Anwendung angezeigt:

   - 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.

   Mit den Schaltflächen **Export**, die sich im oberen Bereich eines jeden Abschnitts befinden, können Sie die in diesem Block angezeigten Statistiken in eine Datei im Textformat exportieren.

Statistiken zur Ausführung der Anwendung in der Verwaltungskonsole anzeigen

So zeigen Sie die Statistiken zur Ausführung der Anwendung 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 Anwendung 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.

   Auf der rechten Seite des Fensters werden die folgenden Ausführungsstatistiken der Anwendung angezeigt:

   - 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.

   Mit den Schaltflächen **Export**, die sich unterhalb eines jeden Abschnitts befinden, können Sie die in diesem Block angezeigten Statistiken in eine Datei im Textformat exportieren.

Liste mit Mountpunkten in der Web Console anzeigen

So zeigen Sie die Liste mit Mountpunkten in der Web Console an:

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

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** oberhalb der Liste der verwalteten Geräte und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

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

3. Suchen Sie in der Liste das Gerät, für das Sie Informationen anzeigen möchten, und klicken Sie auf den Gerätenamen.

4. 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.

Im Fenster **Mountpunkte** wird eine Tabelle mit den folgenden Spalten angezeigt:

- **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 sich im oberen Teil des Fenster über 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]`.

Liste mit Mountpunkten in der Verwaltungskonsole anzeigen

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 Anwendung 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 → Mountpunkte** aus.

   Auf der rechten Seite des Fensters wird die Tabelle **Liste der Mountpunkte** mit den folgenden Spalten angezeigt:

   - **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]`.

Statistiken zur Ausführung der Anwendung und Liste mit Mountpunkten in der Befehlszeile anzeigen

Führen Sie den folgenden Befehl aus, um die Statistiken zur Ausführung der Anwendung und die Liste mit Mountpunkten anzuzeigen:

```
kesl-control [-S] --get-statistic [--files] [--processes] [--mountpoints]
```

wobei:

- `[--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 Mountpunkte.

  Die Ausgabe zeigt die folgenden Informationen an:

  - `[ausgeschlossen]` 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

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.

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.

Um das Sammeln von Kennzahlen zu Betriebssystemressourcen, die von der Anwendung verwendet werden, zu konfigurieren, führen Sie den folgenden Befehl aus:

```
kesl-control [-J] --export-metrics [--period <Intervall zwischen den Exporten in Sekunden>|--interactive]
```

wobei:

- `--period` – periodisches Intervall für die Ausgabe der Ergebnisse an die Befehlszeile
- `--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 Sensor	Die Anzahl der Handles, die der Prozess "kesl" aktuell geöffnet hat. Wenn die Anzahl der Handles auf über 250 pro Stunde anwächst, wird es empfohlen, 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 Sensor	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 Sensor	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 Sensor	Die Menge des Speichers der Auslagerungsdatei, 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.

Interne Bezeichnung der Metrik, Tag und Typ der Metrik	Beschreibung und empfohlener Schwellenwert
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.
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 Sensor	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 Sensor	Die aktuelle Anzahl der eingehenden, abgefangenen Netzwerkverbindungen in diesem Moment.
lfs_tproxy_connection_count Bezeichnung direction=outbound Sensor	Die aktuelle Anzahl der ausgehenden, abgefangenen Netzwerkverbindungen in diesem Moment.

Interne Bezeichnung der Metrik, Tag und Typ der Metrik	Beschreibung und empfohlener Schwellenwert
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.
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 Sensor	Aktuelle Anzahl der Sockets (Listening-Sockets und Connecting-Sockets). Die abgefangene Verbindung verfügt über 2 Verbindungssockets.
lfs_trafficScanning_object_hanging_count Sensor	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 Sensor	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 Sensor	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.

Interne Bezeichnung der Metrik, Tag und Typ der Metrik	Beschreibung und empfohlener Schwellenwert
lfs_faCache_volume_count Sensor	Aktuelle Größe des Caches der Mountpunkte des fanotify-Interceptors.
lfs_oas_cache_file_count Sensor	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.
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 Sensor	Die aktuelle Größe des Caches der Mountpunkte für den Schutz vor bedrohlichen Dateien.
lfs_processManager_cache_size Sensor	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 Sensor	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_prevention_cache_file_count Sensor	Die aktuelle Größe des Caches der Dateien der Aufgabe zur Ausführungsprävention für Objekte, die nicht untersucht werden müssen.
lfs_prevention_cache_file_hit_count Counter	Die Anzahl der Cache-Treffer der Dateien der Aufgabe zur Ausführungsprävention für Objekte, die nicht untersucht werden müssen.
lfs_prevention_cache_file_miss_count Counter	Die Anzahl der Cache-Fehler der Dateien der Aufgabe zur Ausführungsprävention für Objekte, die nicht überprüft werden müssen.
lfs_prevention_cache_volume_count Sensor	Aktuelle Größe des Caches der Aufgabe zur Ausführungsprävention für Objekte.
eka_telemetry_metrics_registry_callbacks_exec_duration_milliseconds Sensor	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 Sensor	Die aktuelle Anzahl von Funktionsaufrufen zum Kennzahlen-Update, die der MetricsRegistry für alle registrierten Clients durchgeführt hat.
eka_telemetry_metrics_registry_scrape_duration_milliseconds Sensor	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.

Datenbanken und Module der Anwendung aktualisieren

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.

Ein Update der Datenbanken und Module von Kaspersky Endpoint Security gewährleistet, dass der Schutz des Geräts auf dem neuesten Stand ist. Weltweit tauchen praktisch täglich neue Viren, Schadsoftware und andere Programme auf, die eine Bedrohung darstellen. Die Datenbanken der Anwendung enthalten Informationen über Bedrohungen und Möglichkeiten für deren Neutralisierung. Um Bedrohungen rasch erkennen zu können, müssen Sie die Datenbanken und Module der Anwendung 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.

Während des Update-Vorgangs werden Datenbanken und Module der Anwendung heruntergeladen und auf Ihrem Gerät installiert. Sie können Updates für die Datenbanken und Module der Anwendung von den Update-Servern von Kaspersky, aus der Datenverwaltung des Administrationsservers, aus lokalen oder Netzwerkverzeichnissen und von anderen Update-Quellen erhalten.

Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, wird das Verzeichnis auf der SVM als Update-Quelle verwendet.

Während des Updates werden die Module und die Datenbanken der Anwendung auf Ihrem Gerät mit der aktuellen Version in der Update-Quelle verglichen. Wenn Ihre aktuellen Datenbanken und Module der Anwendung 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.

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 in den allgemeinen Anwendungseinstellungen an.

Unabhängig von der Update-Quelle erfolgt das Herunterladen des Update-Pakets und die Installation von Updates für die Datenbanken und Module der Anwendung auf dem Gerät mithilfe der Aufgabe *Update*. Die Anwendung erstellt eine vordefinierte Aufgabe vom Typ *Update*. Mit dieser Aufgabe können Sie die Datenbanken und Module der Anwendung nach einem Zeitplan und auf Befehl aktualisieren und Update-Einstellungen konfigurieren.

Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, werden die Datenbanken auf geschützten virtuellen Maschinen mithilfe einer speziellen und lokalen Aufgabe *Update* aktualisiert, bei welcher als Update-Quelle ein Verzeichnis auf der SVM angegeben wurde. Diese Update-Aufgabe wird automatisch gestartet. Sie können diese Aufgabe weder löschen noch ihre Einstellungen ändern. Das Aktualisieren von Datenbanken und Modulen der Anwendung mithilfe von Aufgaben, die in Kaspersky Security Center erstellt wurden, wird nicht unterstützt.

Wenn Kaspersky Endpoint Security im Standard-Modus oder im Modus als Endpoint Detection and Response Agent verwendet wird, können Sie in Kaspersky Security Center die Gruppenaufgabe *Update* verwenden, die der Assistent für die Erstkonfiguration nach der Installation des MMC-Plug-ins oder des Web-Plug-ins für die Verwaltung von Kaspersky Endpoint Security erstellt. Sie können Benutzeraufgaben für Updates auch über die Befehlszeile und in Kaspersky Security Center erstellen.

Sie können die folgenden Einstellungen für die Aktualisierung der Datenbanken und Module der Anwendung konfigurieren:

- Wählen Sie je nach verwendetem Update-Szenario die Quelle aus, aus der die Anwendung die Updates erhalten soll.
- Konfigurieren Sie die Wartezeit auf eine Antwort von der ausgewählten Update-Quelle beim Versuch, eine Verbindung herzustellen. Wenn in der angegebenen Zeit keine Antwort von der Update-Quelle eingeht, greift die Anwendung auf eine andere angegebene Update-Quelle zu.
- Konfigurieren Sie den Zeitplan für den Start der Update-Aufgabe. Standardmäßig aktualisiert die Anwendung die Datenbanken einmal alle 60 Minuten.

Sie können auch automatisch installierbare Anwendungsupdates (Autopatches) abrufen. In den Einstellungen der Update-Aufgabe können Sie den Modus für das Herunterladen und Installieren von Autopatches auswählen: "Herunterladen und installieren", "Nur herunterladen" oder "Nicht herunterladen".

Informationen zum Aktualisieren von Datenbanken und Modulen

Während der Durchführung eines Updates werden die folgenden Objekte heruntergeladen und auf Ihrem Gerät installiert:

- Anwendungsdatenbanken. Zu den App-Datenbanken gehören Datenbanken mit Signaturen von Schadsoftware, Beschreibungen von Netzwerkangriffen, Datenbanken mit bösartigen Webadressen und Phishing-Adressen, Datenbanken mit Bannern, Spam-Datenbanken und andere Daten.

  Wenn die Aktualisierung der Datenbanken auf dem Gerät unterbrochen wird oder mit einem Fehler fehlschlägt, verwendet die Anwendung weiterhin die zuvor installierte Version der Datenbanken. Wenn bisher noch keine Anwendungsdatenbanken installiert wurden, wird die Anwendung im Modus "ohne Datenbanken" ausgeführt. Die Aktualisierung der Datenbanken und Module der Anwendung ist weiterhin verfügbar.

Wenn das Datenbanken-Update erfolgreich abgeschlossen wurde, die Datenbanken jedoch beschädigt sind und die Anwendung mehrmals hintereinander fehlerhaft beendet wird, werden die Datenbanken automatisch gelöscht. Die Anwendung wird weiterhin im Modus "ohne Datenbanken" ausgeführt. Das Update der Datenbanken und Anwendungsmodule ist weiterhin verfügbar.

Die Datenbank ist aktuell, wenn sie vor weniger als 3 Tagen herunterladen wurde. Standardmäßig generiert die App das Ereignis *Programmdatenbanken sind veraltet*, wenn die zuletzt installierten Datenbanken-Updates vor mehr als drei, aber weniger als sieben Tagen auf den Kaspersky-Servern veröffentlicht wurden. Wenn die Datenbanken seit sieben Tagen nicht aktualisiert wurden, generiert die App das Ereignis *Programmdatenbanken sind völlig veraltet*.

- App-Module. Modul-Updates dienen dazu, Schwachstellen in der Anwendung zu beseitigen und die Schutztechniken für das Gerät zu verbessern. Modul-Updates können das Verhalten von Anwendungskomponenten anpassen und neue Funktionen hinzufügen.

  Ein Update der Anwendung kann unabhängig vom Status der Anwendung (gestartet, gestoppt, durch eine Richtlinie von Kaspersky Security Center verwaltet) und dem Update-Zeitplan installiert werden. Während eines Updates der Anwendungsmodule setzt Kaspersky Endpoint Security den Schutz Ihres Gerätes fort. Während eines Updates werden die Einstellungen der Anwendung und das Ereignisprotokoll der Anwendung auf die neue Anwendungsversion übertragen.

  Wenn die Übertragung der Einstellungen aus irgendeinem Grund fehlschlägt, wird die Anwendung auf die Standardwerte zurückgesetzt.

  Änderungen an den Anwendungseinstellungen, die Sie nach Abschluss der Aktualisierung und vor dem Neustart der Anwendung vornehmen, werden nicht gespeichert.

  Wenn die Anwendung nach einem Update nicht ordnungsgemäß funktioniert, wird sie automatisch auf die vorherige Version zurückgesetzt. Es wird empfohlen, Kontakt mit dem Technischen Support von Kaspersky aufzunehmen.

Informationen zu Update-Quellen und -Szenarien

Update-Quelle – Eine Ressource, die Datenbanken-Updates und Updates der Module der Anwendung Kaspersky Endpoint Security enthält. Als Update-Quelle können FTP-, HTTP- oder HTTPS-Server (z. B. die Update-Server von Kaspersky) sowie lokale Verzeichnisse und Netzwerkverzeichnisse dienen, die von den Benutzern gemountet sind.

Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, werden Datenbanken auf geschützten virtuellen Maschinen aus dem Verzeichnis auf der SVM aktualisiert.

Als primäre Update-Quelle dienen die Kaspersky-Update-Server. Sie können andere Update-Quellen in den Einstellungen der Aufgabe *Update* angeben. Wenn ein Update aus einer bestimmten Update-Quelle nicht durchgeführt werden kann, verbindet sich Kaspersky Endpoint Security mit der nächsten Quelle.

Die Anwendung Kaspersky Endpoint Security unterstützt die folgenden Szenarien für das Update von Datenbanken und Modulen:

- Update von den Kaspersky-Update-Servern Die Kaspersky-Update-Server befinden sich in verschiedenen Ländern auf der ganzen Welt, was eine hohe Zuverlässigkeit der Updates gewährleistet. Wenn ein Update von einem bestimmten Server aus nicht durchgeführt werden kann, wechselt die Anwendung zum nächsten Server. Die Updates werden über das HTTPS-Protokoll heruntergeladen.

- Zentralisiertes Update Das zentralisierte Update reduziert den externen Internet-Datenverkehr und ermöglicht eine bequeme Überwachung 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 von der Aufgabe des Administrationsservers *Download von Updates in die Datenverwaltung des Administrationsservers* in die Datenverwaltung des Administrationsservers heruntergeladen.

   Wenn Sie die Anwendung mit der Kaspersky Security Center Cloud Console verwalten, können Sie den Speicher von Verteilungspunkten (Geräte, auf denen der Administrationsagent installiert ist) als Speicher verwenden. Nähere Informationen über Verteilungspunkte finden Sie in der Hilfe zu Kaspersky Security Center.

2. Verteilen Sie das Update-Paket an die Client-Geräte.

   Das Update-Paket wird von der *Update*-Aufgabe der Anwendung Kaspersky Endpoint Security an die Client-Geräte verteilt. In den Aufgabeneinstellungen müssen Sie "Kaspersky Security Center" als Update-Quelle festlegen.

- Aktualisierung aus einem lokalen Verzeichnis oder Netzwerkverzeichnis (SMB/NFS), das vom Benutzer gemountet wurde, oder von einem FTP-, HTTP- oder HTTPS-Server. Sie können eine benutzerdefinierte Update-Quelle in den Einstellungen der Aufgabe *Update* angeben.

Datenbanken und Module der Anwendung in der Web Console aktualisieren

In der Web Console können Sie die Datenbanken und Module der Anwendung mithilfe der Aufgabe *Update* aktualisieren. Sie können die automatisch erstellte Gruppenaufgabe *Update* verwenden und auch Benutzeraufgaben für Updates erstellen.

So konfigurieren Sie Update-Einstellungen in der Web Console:

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

   Die Aufgabenliste wird geöffnet.

2. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf allen Geräten einer bestimmten Administrationsgruppe ausgeführt wird, klicken Sie auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

     In der Liste werden nur die Aufgaben angezeigt, die für die ausgewählte Administrationsgruppe konfiguriert sind.

   - Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf einem oder mehreren Geräten ausgeführt wird (Aufgaben für eine Gerätegruppe), klicken Sie auf den Link im Feld **Aktueller Pfad** oben im Fenster und wählen Sie im angezeigten Fenster den oberen Knoten mit dem Namen des Administrationsservers.

     In der Liste werden alle auf dem Administrationsserver erstellten Aufgaben angezeigt.

3. Wählen Sie in der Aufgabenliste die erforderliche **Update**-Aufgabe aus und öffnen Sie über den Link im Aufgabennamen das Fenster mit den Aufgabeneigenschaften.

4. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Programmeinstellungen** aus. Wählen Sie in der Liste links den Abschnitt **Update-Quellen** aus.

5. 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.

6. Wählen Sie den Abschnitt **Einstellungen** aus und konfigurieren Sie die weiteren Update-Einstellungen.

7. Wählen Sie die Registerkarte **Zeitplan** aus und konfigurieren Sie den Zeitplan für den Start der Update-Aufgabe.

   Wenn Sie **Kaspersky Security Center** als Update-Quelle ausgewählt haben, wählen Sie in der Dropdown-Liste **Aufgabenstart** die Option **Wenn Updates in den Speicher heruntergeladen werden** aus. Nähere Informationen über Aufgabenzeitpläne finden Sie in der Hilfe zu Kaspersky Security Center.

8. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die Aufgabe wird gemäß dem konfigurierten Zeitplan gestartet. Sie können die Aufgabe auch manuell starten.

Abschnitt "Update-Quellen für die Update-Aufgabe"

Parameter	Description

Tabelle der Update-Quellen	Diese Tabelle enthält eine Liste mit den Quellen für die Datenbanken-Updates. Während des Updates wendet sich die Anwendung der Reihe nach so an die Update-Quellen, wie sie in der Tabelle platziert wurden.
	Folgende Spalten sind in der Tabelle enthalten:
	• **Update-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 (**Aktiviert** bzw. **Deaktiviert**). Sie können den Status auf zwei Arten ändern: über den Umschalter in der Tabelle oder über den Umschalter **Diese Quelle verwenden** der im Fenster **Update-Quelle** angezeigt wird, wenn Sie auf den Link mit dem Namen der Quelle klicken.
	Sie können Update-Quellen in der Tabelle **hinzufügen**, **bearbeiten**, löschen, **nach oben verschieben** oder **nach unten verschieben**.
	Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.
	Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.
	Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.
	Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.
	Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.
	Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Abschnitt "Einstellungen der Update-Aufgabe"

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

Parameter	Description
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.

Datenbanken und Module der Anwendung in der Verwaltungskonsole aktualisieren

In der Verwaltungskonsole können Sie die Datenbanken und Module der Anwendung mithilfe der Aufgabe *Update* aktualisieren. Sie können die automatisch erstellte Gruppenaufgabe *Update* verwenden und auch Benutzeraufgaben für Updates erstellen.

So konfigurieren Sie Update-Einstellungen in der Verwaltungskonsole:

1. Führen Sie in der Verwaltungskonsole eine der folgenden Aktionen aus:

   - Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf Geräten ausgeführt wird, die zu einer bestimmten Administrationsgruppe gehören, wählen Sie diese Administrationsgruppe in der Konsolenstruktur aus und wählen Sie dann im Arbeitsbereich die Registerkarte **Aufgaben** aus.

   - Wenn Sie die Einstellungen einer Aufgabe ändern möchten, die auf einem oder mehreren Geräten ausgeführt wird (Aufgaben für eine Gerätegruppe), wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.

2. Wählen Sie in der Aufgabenliste die erforderliche **Update**-Aufgabe aus und öffnen Sie das Eigenschaftenfenster der Aufgabe mit einem Doppelklick.

3. Wählen Sie im Eigenschaftenfenster der Aufgabe in der Liste links den Abschnitt **Update-Quellen** aus.

4. Wählen Sie 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 den Abschnitt **Zeitplan** aus und konfigurieren Sie den Zeitplan für den Start der Update-Aufgabe.

   Wenn Sie **Kaspersky Security Center** als Update-Quelle ausgewählt haben, wählen Sie in der Dropdown-Liste **Geplanter Start** die Option **Wenn Updates in den Speicher heruntergeladen werden** aus. Nähere Informationen über Aufgabenzeitpläne finden Sie in der Hilfe zu Kaspersky Security Center.

7. Klicken Sie im Fenster **Eigenschaften: <Aufgabenname>** auf die Schaltfläche **Übernehmen** oder die Schaltfläche **OK**, um die Änderungen zu speichern.

Die Aufgabe wird gemäß dem konfigurierten Zeitplan gestartet. Sie können die Aufgabe auch manuell starten.

Abschnitt "Update-Quellen für die Update-Aufgabe"

Parameter	Description

Update-Quelle	Diese Tabelle enthält eine Liste mit den Quellen für die Datenbanken-Updates. Während des Updates wendet sich die Anwendung 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 verschieben** oder **nach unten verschieben**.
	Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.
	Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.
	Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.
	Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.
	Die Änderung der Parameter des ausgewählten Elements erfolgt in einem separaten Fenster.
	Ein Klick auf die Schaltfläche **Hinzufügen** öffnet ein Fenster, in dem Sie die Einstellungen des neuen Elements anpassen können.

Abschnitt "Einstellungen der Update-Aufgabe"

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.

Datenbanken und Module der Anwendung über die Befehlszeile aktualisieren

In der Befehlszeile können Sie die Datenbanken und Module der Anwendung auf folgende Arten aktualisieren:

- Mithilfe der vordefinierten Update-Aufgabe (*Update*). Sie können diese Aufgabe manuell starten, beenden, anhalten und fortsetzen und den Zeitplan für den Aufgabenstart konfigurieren. Sie können die Update-Einstellungen verwalten, indem Sie die Einstellungen dieser Aufgabe ändern.

- Mithilfe von Benutzeraufgaben für Updates (Aufgaben vom Typ *Update*). Sie können Benutzeraufgaben manuell starten und den Zeitplan für den Aufgabenstart konfigurieren.

Einstellungen der Update-Aufgabe

Parameter	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 im Parameter `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 Anwendung 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. `Benutzerdefiniert` Das Programm 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.

Update mithilfe von Kaspersky Update Utility

Um den Internetverkehr zu reduzieren, können Sie auf den Geräten im lokalen Unternehmensnetzwerk das Update von Datenbanken und Modulen der Anwendung 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 die Eigenschaften der Aufgabe **Update**, die auf dem erforderlichen Gerät ausgeführt werden soll, über Web Console oder über die Verwaltungskonsole.

   b. Wechseln Sie in den Aufgabeneigenschaften zum Abschnitt **Update-Quellen**.

   c. Wählen Sie im Block **Update-Quellen** die Option **Andere Quellen im lokalen oder globalen Netzwerk** aus.

   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 der Organisation: 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.

Rollback von Datenbanken- und Modul-Updates durchführen

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, wird das Rollback des Datenbanken-Updates mittels einer Aufgabe nicht unterstützt.

Nach dem erstmaligen Update der Anwendungsdatenbanken wird die Rollback-Funktion verfügbar, mit der die Anwendungsdatenbanken auf eine frühere Version zurückgesetzt werden können.

Jedes Mal, wenn der Benutzer den Update-Vorgang startet, erstellt die Anwendung Kaspersky Endpoint Security eine Backup-Kopie der aktuellen Anwendungsdatenbanken. Auf diese Weise können Sie bei Bedarf die Anwendungsdatenbanken auf eine frühere Version zurücksetzen.

Das Rollback des letzten Datenbanken-Updates ist z. B. dann sinnvoll, wenn die neue Version der Anwendungsdatenbanken eine ungültige Signatur enthält, weswegen die Anwendung Kaspersky Endpoint Security eine sichere Anwendung blockiert.

In der Befehlszeile zum Rollback von Updates können Sie die vordefinierte Aufgabe zum *Rollback des Datenbank-Updates (Rollback)* starten oder benutzerdefinierte Aufgaben zum Rollback von Updates (Aufgaben des Typs *Rollback*) erstellen und ausführen.

In Kaspersky Security Center können Sie über Web Console oder über die Verwaltungskonsole Update-Rollback-Aufgaben für Administrationsgruppen oder einzelne Geräte erstellen.

Die Aufgabe *Rollback des Datenbanken-Updates* hat keine Einstellungen.

Schutz vor bedrohlichen Dateien

Die Komponente "Schutz vor bedrohlichen Dateien" verhindert eine Infektion des Dateisystem des Geräts. Die Komponente wird beim Start von Kaspersky Endpoint Security automatisch mit den Standardeinstellungen aktiviert. Sie befindet sich im Arbeitsspeicher des Geräts und untersucht in Echtzeit alle Dateien, die geöffnet, gespeichert und gestartet werden.

Wenn Schadsoftware entdeckt wird, kann Kaspersky Endpoint Security die infizierte Datei löschen und den von dieser Datei gestarteten schädlichen Prozess beenden.

Der Modus des Interceptors von Dateioperationen, den Sie in den allgemeinen Anwendungseinstellungen auswählen können, wirkt sich auf die Ausführung der Komponente aus. Während der Untersuchung wird der Zugriff auf eine Datei standardmäßig blockiert.

Wenn ein Benutzer mit root-Berechtigung keinen Zugriff auf eine Datei in einem über NFS4 eingebundenen Remote-Verzeichnis hat, blockiert die Anwendung den Zugriff auf die Datei für alle Benutzer.

Wenn der Schutz vor bedrohlichen Dateien und die Container-Überwachung (Untersuchung von Containern, Container-Überwachung) aktiviert sind, untersucht die App auch alle Namespaces und Container auf allen unterstützten Betriebssystemen.

Sie können den Schutz vor bedrohlichen Dateien ein- und ausschalten und auch Schutzeinstellungen konfigurieren:

- Wählen Sie den Modus für die Untersuchung von Dateien aus (beim Öffnen, beim Öffnen und Ändern).
- Aktivieren und deaktivieren Sie die Untersuchung von Archiven, E-Mail-Datenbanken und E-Mail-Nachrichten im Textformat.
- Schließen Sie Dateien im Textformat vorübergehend aus der erneuten Untersuchung aus.
- Begrenzen Sie die Größe des untersuchten Objekts und die Untersuchungsdauer für das Objekt.
- Wählen Sie die Aktionen aus, welche die Anwendung für infizierte Objekte ausführen soll.
- Konfigurieren Sie den *Untersuchungsbereich*. Die Anwendung untersucht Objekte im angegebenen Bereich des Dateisystems.
- Konfigurieren Sie den Ausschluss von Objekten aus der Untersuchung. Eine *Untersuchungsausnahme* ist eine Reihe von Bedingungen. Wenn diese Bedingungen erfüllt sind, untersucht das Programm die Objekte nicht auf Viren und andere Malware. Sie können Folgendes von der Untersuchung ausschließen:
  - Objekte nach Namen oder Masken.
  - Objekte nach dem Namen der in den Objekten gefundenen Bedrohungen.
  - Dateien und Verzeichnisse in bestimmten Bereichen des Dateisystems.
  - Prozesse und Dateien, die durch den angegebenen Prozess geändert wurden.

Die Anwendung schließt außerdem automatisch bestimmte interne Prozesse von der Untersuchung aus, beispielsweise den Prozess des Watchdog-Servers.

- Konfigurieren Sie die Verwendung der heuristischen Analyse und der iChecker-Technologie während der Untersuchung.
- Aktivieren und deaktivieren Sie die Protokollierung von Informationen zu untersuchten nicht infizierten Objekten, zu untersuchten Objekten in Archiven und zu nicht verarbeiteten Objekten.

Um die Ausführung der Komponente zum Schutz vor bedrohlichen Dateien zu optimieren, können Sie den Ausschluss von Dateien, die aus Netzwerkverzeichnissen kopiert wurden, von der Untersuchung konfigurieren. Dateien werden erst untersucht, nachdem das Kopieren in das lokale Verzeichnis abgeschlossen ist. Um Dateien in Netzwerkverzeichnissen von der Untersuchung auszuschließen, müssen Sie für ein Tool, das zum Kopieren aus Netzwerkverzeichnissen bestimmt ist (z. B. für das Tool `cp`) einen Ausschluss nach Prozess konfigurieren. Wenn Sie die 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 `Einstellungen für OAS-Aufgaben hinzufügen`.

Schutz vor bedrohlichen Dateien in der Web Console konfigurieren

In der Web Console können Sie die Einstellungen des Schutzes vor bedrohlichen Dateien in den Richtlinieneigenschaften konfigurieren (**Anwendungseinstellungen** → **Host-Schutz** → **Schutz vor bedrohlichen Dateien**).

Schutz vor bedrohlichen Dateien in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen für den Schutz vor bedrohlichen Dateien in den Eigenschaften der Richtlinie verwalten (Verwalten von Richtlinien in der Verwaltungskonsole, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Basisschutz** → **Schutz vor bedrohlichen Dateien**).

Einstellungen der Komponente zum 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.

Parameter	Description
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.

Einstellungen des Untersuchungsbereichs

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 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 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.

Parameter	Description
	Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Untersuchungsbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie **Masken** und **Tags** verwenden. Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben: • `[container-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` Wobei gilt: `<ID>` ist die Container-ID. `<Name>` ist ein Containername `<Pfad zum lokalen Verzeichnis>` 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>]/Pfad zum lokalen Verzeichnis>`. Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert. Beispiel: • `[container-name:<Name>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` • `[container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>][image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][image-id:<ID>][container-id:<ID>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardmäßige Pfadangabe **/** – Die 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.

Fenster "Untersuchungseinstellungen"

In diesem Fenster können Sie die Einstellungen für die Untersuchung von Dateien durch den Schutz vor bedrohlichen Dateien konfigurieren.

Einstellungen für den Schutz vor bedrohlichen Dateien

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.

Parameter	Description
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.
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 bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung 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 Richtlinieneigenschaften verwalten (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Basisschutz → Ausnahmen für den Schutz 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 Anwendung untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden.

Einstellungen des Ausschlussbereichs

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 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 Ausschlussbereich>

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.

Parameter	Description
	Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Ausschlussbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie **Masken** und **Tags** verwenden. Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben: • `[container-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` Wobei gilt: `<ID>` ist die Container-ID. `<Name>` ist ein Containername `<Pfad zum lokalen Verzeichnis>` 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>]/Pfad zum lokalen Verzeichnis>`. Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert. Beispiel: • `[container-name:<Name>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` • `[container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>][image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][image-id:<ID>][container-id:<ID>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Als Pfad ist standardmäßig **/** angegeben. Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus.
Name des Dateisystems	Eingabefeld für den Namen des Dateisystems, auf dem sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste auf der rechten Seite das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der 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.

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).

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.

Parameter	Description
Pfad zu den geänderten Dateien	Diese Einstellungsgruppe erlaubt, Ausschlüsse von der Untersuchung für Dateien festzulegen, die der Prozess verändert. In der Dropdown-Liste der Dateisysteme können Sie den Typ des Dateisystems auswählen, auf dem sich die Verzeichnisse befinden, die von der Untersuchung ausgeschlossen werden sollen: • **Lokal** – Lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie den Pfad zu einem lokalen Verzeichnis angeben. • **Mounted** – Gemountete Remote-Verzeichnisse oder lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie das Protokoll oder den Namen des Dateisystems angeben. • **Freigegeben** – Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind. • **Alle freigegebenen** – Alle Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind.
	Wenn in der Dropdown-Liste der Dateisysteme **Mounted** oder **Alle** ausgewählt ist, können Sie in der Dropdown-Liste der Zugriffsprotokolle das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind.
	Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Ausschlussbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie **Masken** verwenden. Das Eingabefeld darf nicht leer sein. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.
Name des Dateisystems	Eingabefeld für den Namen des Dateisystems, auf dem sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste auf der rechten Seite das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der 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.

Schutz vor bedrohlichen Dateien über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie den Schutz vor bedrohlichen Dateien mithilfe der vordefinierten Aufgabe "Schutz vor bedrohlichen Dateien" (*File_Threat_Protection*) verwalten.

Die Aufgabe "Schutz vor bedrohlichen Dateien" wird standardmäßig gestartet. Sie können diese Aufgabe manuell starten und beenden.

Die Rechte der Administrator-Rolle sind erforderlich, um die Aufgabe zum Schutz vor bedrohlichen Dateien über die Befehlszeile zu starten und zu beenden.

Sie können die Einstellungen für den Schutz vor bedrohlichen Dateien konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zum Schutz vor bedrohlichen Dateien ändern.

Einstellungen der Aufgabe zum Schutz vor bedrohlichen Dateien

Die Tabelle beschreibt alle möglichen Werte sowie die Standardwerte aller Einstellungen, die Sie für die Aufgabe zum Schutz vor bedrohlichen Dateien angeben 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 Textformat untersuchen. `No` (Standardwert) – E-Mail-Nachrichten im Textformat nicht untersuchen.
`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.

Parameter	Description	Werte
`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`.
`UseExcludeMasks`	Aktiviert den Ausschluss von Objekten, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, von der Untersuchung.	`Yes` – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, aus der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht aus der 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.*`

Parameter	Description	Werte
`UseExcludeThreats`	Ermöglicht es, für Objekte, die die durch die Einstellung `ExcludeThreats.item_#` festgelegten Bedrohungen enthalten, Ausnahmen von Untersuchungen zu erstellen.	`Ja` — Objekte, die 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 Anwendung 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 die Untersuchung von Objekten, die zu einem Archiv gehören, im Protokoll speichern. `No` (Standardwert) – Informationen über die Untersuchung von Objekten, die zu einem Archiv gehören, nicht im Protokoll speichern.
`ReportUnprocessedObjects`	Aktiviert das Protokollieren von Informationen über Objekte, die aus einem bestimmten Grund nicht verarbeitet wurden.	`Yes` – Informationen zu nicht verarbeiteten Objekten im Protokoll speichern. `No` (Standardwert) – Informationen zu nicht verarbeiteten Objekten nicht im Protokoll speichern.
`UseAnalyzer`	Aktiviert die heuristische Analyse. 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.

Parameter	Description	Werte
`HeuristicLevel`	Legt die Stufe der heuristischen Analyse fest. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Gründlichkeit der Suche nach Bedrohungen, der Belastung der Betriebssystemressourcen und der Untersuchungsdauer. Je höher die festgelegte Ebene der heuristischen Analyse, desto mehr Ressourcen verbraucht die Untersuchung und desto länger dauert sie.	`Light` – Oberflächlichste Untersuchung mit minimaler Belastung des Systems. `Medium` – Mittlere Ebene der heuristischen Analyse mit ausgeglichener Belastung des Betriebssystems. `Deep` – Gründlichste Untersuchung mit maximaler Belastung des Betriebssystems. `Recommended` (Standardwert) – Der empfohlene Wert.
`UseIChecker`	Aktiviert die Nutzung der iChecker-Technologie.	`Yes` (Standardwert) – Nutzung der iChecker-Technologie aktivieren. `No` – Nutzung der iChecker-Technologie deaktivieren.
`ScanByAccessType`	Ausführungsmodus der Aufgabe zum Schutz vor bedrohlichen Dateien. Die Einstellung `ScanByAccessType` wird nur in der Aufgabe zum Schutz vor bedrohlichen Dateien verwendet.	`SmartCheck` (Standardwert) – die Datei wird beim Öffnen und erneut beim Schließen untersucht, falls sie geändert wurde. Wenn ein Prozess während seiner Ausführung in einem bestimmten Zeitraum mehrmals auf die Datei zugreift und diese verändert, wird diese Datei erst beim letzten Versuch des Prozesses, die Datei zu schließen, untersucht. `OpenAndModify` – die Datei wird beim Öffnen und erneut beim Schließen untersucht, falls sie geändert wurde. `Open` – die Datei wird beim Öffnen zum Lesen sowie beim Ausführen oder Ändern untersucht.
Der Abschnitt **[ScanScope.item_#]** enthält die folgenden Parameter:		
`AreaDesc`	Beschreibung des Untersuchungsbereichs, der erweiterte Informationen über den Untersuchungsbereich enthält. Die maximale Länge einer Zeichenfolge, die mit dieser Einstellung angegeben werden kann, beträgt 4096 Zeichen.	Standardwert: `All objects` Beispiel: `AreaDesc=" Mail-Datenbanken untersuchen "`
`UseScanArea`	Aktiviert die Untersuchung des angegebenen Bereichs. Um die Aufgabe auszuführen, müssen Sie mindestens einen zu untersuchenden Bereich angeben.	`Yes` (Standardwert) – Den angegebenen Bereich untersuchen. `No` – Angegebenen Bereich nicht untersuchen.
`AreaMask.item_#`	Einschränkung des Untersuchungsbereichs. Im Untersuchungsbereich untersucht die 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_< Nummer des Elements >=*doc`

Parameter	Description	Werte
`Path`	Pfad zum Verzeichnis mit untersuchten Objekten.	`< Pfad zum lokalen Verzeichnis >` — Objekte im angegebenen Verzeichnis untersuchen. Bei der Angabe des Pfades können Sie **Masken** und **Tags** verwenden. Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben: • `[container-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` Wobei gilt: `<ID>` ist die Container-ID. `<Name>` ist ein Containername `<Pfad zum lokalen Verzeichnis>` 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>]/Pfad zum lokalen Verzeichnis>`. Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert. Beispiel: • `[container-name:<Name>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` • `[container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>][image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][image-id:<ID>][container-id:<ID>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. `Shared:NFS` – Ressourcen des Gerätedateisystems untersuchen, auf die über das NFS-Protokoll zugegriffen wird. `Shared:SMB` – Ressourcen des Gerätedateisystems untersuchen, auf die über das Samba-Protokoll zugegriffen wird. `Mounted:NFS` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über NFS-Protokoll eingebunden sind. `Mounted:SMB` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über das Samba-Protokoll eingebunden sind.

Parameter	Description	Werte
		`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. `<Dateisystemtyp>` – Alle Ressourcen des angegebenen Dateisystemgeräts untersuchen.
Der Abschnitt **[ExcludedFromScanScope.item_#]** enthält die folgenden Parameter:		
`AreaDesc`	Beschreibung des Ausschlussbereichs, der erweiterte Informationen über den Ausschlussbereich enthält.	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 Anwendung nur Dateien, die mit Masken im Shell-Format angegeben wurden. Wenn die Einstellung nicht angegeben wurde, schließt die Anwendung alle Objekte im Ausschlussbereich von der Untersuchung aus. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: `*` (alle Objekte von der Untersuchung ausschließen)

Parameter	Description	Werte
`Path`	Pfad zum Verzeichnis mit ausgeschlossenen Objekten.	`< Pfad zum lokalen Verzeichnis >` – Objekte im angegebenen Verzeichnis (einschließlich Unterverzeichnissen) von Untersuchungen ausschließen. Bei der Angabe des Pfades können Sie **Masken** und **Tags** verwenden. Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben: • `[container-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` Wobei gilt: `<ID>` ist die Container-ID. `<Name>` ist ein Containername `<Pfad zum lokalen Verzeichnis>` 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>]/Pfad zum lokalen Verzeichnis>`. Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert. Beispiel: • `[container-name:<Name>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` • `[container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>][image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][image-id:<ID>][container-id:<ID>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. `Mounted:NFS` – Remote-Verzeichnisse, 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.

Parameter	Description	Werte
		`<Typ des Dateisystems>` – alle Ressourcen des angegebenen Dateisystems des Geräts 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.	`< vollständiger Pfad zum Prozess >` – Prozess im angegebenen lokalen Verzeichnis nicht untersuchen.
`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.	Standardwert: `All objects`
`UseExcludedForProgram`	Schließt den angegebenen Bereich von der Untersuchung aus.	`Yes` (Standardwert) – Den angegebenen Bereich ausschließen. `No` – Den angegebenen Bereich nicht ausschließen.
`AreaMask.item_#`	Einschränkung des Ausschlussbereichs von Prozessen. Im Ausschlussbereich für Prozesse werden von der Anwendung nur die Dateien nicht untersucht, die mithilfe von Masken im Shell-Format angegeben wurden. Wenn kein Parameter angegeben wurde, werden von der Anwendung alle Objekte im Ausschlussbereich von der Untersuchung ausgeschlossen. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: `*` (alle Objekte von der Untersuchung ausschließen)

Parameter	Description	Werte
`Path`	Pfad des Verzeichnisses mit Dateien, die der Prozess ändert.	`< Pfad zum lokalen Verzeichnis >` schließt Objekte im angegebenen Verzeichnis von der Untersuchung aus. Bei der Angabe des Pfades können Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. `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. `<Dateisystemtyp>` – Alle Ressourcen des angegebenen Dateisystemgeräts von der Untersuchung ausschließen.

Optimierung der Überprüfung von Netzwerkverzeichnissen

Um die Ausführung des Schutzes vor bedrohlichen Dateien zu optimieren, können Sie den Ausschluss von Dateien, die aus Netzwerkverzeichnissen kopiert wurden, von der Untersuchung konfigurieren. Dazu müssen Sie einen Ausschluss nach Prozess für das Tool konfigurieren, das zum Kopieren aus Netzwerkverzeichnissen bestimmt ist (z. B. für das Tool `cp`).

So konfigurieren Sie den Ausschluss von Netzwerkverzeichnissen aus der Untersuchung:

1. Geben Sie die Paramater der Aufgabe "Schutz vor bedrohlichen Dateien" (*File_Threat_Protection*, ID:1) mit dem folgenden Befehl in der Konfigurationsdatei aus:

   ```
   kesl-control --get-settings 1 --file < vollständiger Pfad der Konfigurationsdatei > [--json]
   ```

2. Öffnen Sie die Konfigurationsdatei und fügen Sie den Abschnitt `[ExcludedForProgram.item_#]` mit den folgenden Einstellungen hinzu:

   - `ProgramPath` – Pfad des auszuschließenden Prozesses oder eines Verzeichnisses mit auszuschließenden Prozessen.
   - `ApplyToDescendants` – Einstellung, die angibt, ob untergeordnete Prozesse von der Untersuchung des auszuschließenden Prozesses auszuschließen sind (mögliche Werte: `Yes` oder `No`).
   - `AreaDesc` – Beschreibung des Ausschlussbereichs für Prozesse, die zusätzliche Informationen zum Ausschlussbereich enthält.
   - `UseExcludedForProgram` – Ausschluss des angegebenen Bereichs aktivieren, wenn die Aufgabe ausgeführt wird (mögliche Werte: `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 Befehl aus:

   `kesl-control --set-settings 1 --file <vollständiger Pfad der Konfigurationsdatei> [--json]`

   Geben Sie den Schalter `--json` an, wenn Sie Einstellungen aus einer Konfigurationsdatei im JSON-Format importieren. Wenn Sie keinen Schalter angeben, versucht die 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.

Besonderheiten der Untersuchung von symbolischen Links und festen Links

Kaspersky Endpoint Security ermöglicht die Untersuchung symbolischer und fester Links zu Dateien.

Untersuchung von symbolischen Links

Die Anwendung untersucht symbolische Links nur dann, wenn die Datei, auf die der symbolische Link verweist, zum Untersuchungsbereich der Komponente zum Schutz vor bedrohlichen Dateien gehört.

Wenn die vom symbolischen Link referenzierte Datei nicht in dem Untersuchungsbereich der Komponente zum Schutz vor bedrohlichen Dateien fällt, führt die Anwendung keine Untersuchung dieser Datei durch. Sollte die Datei jedoch bösartigen Code enthalten, ist die Sicherheit des Geräts gefährdet.

Untersuchung von festen Links

Bei Verarbeitung einer Datei mit mindestens einem festen Link wird die ursprüngliche Datei von der Anwendung desinfiziert. Wenn keine Desinfektion möglich ist, löscht die Anwendung den festen Link und erstellt stattdessen eine Kopie der Quelldatei mit dem Namen des entfernten festen Links. Bei der Löschung entfernt die Anwendung den verarbeiteten festen Link. Weitere feste Links zu dieser Datei werden nicht verarbeitet.

Wenn Sie die Datei mit dem festen Link aus dem Backup wiederherstellen, erstellt die Anwendung eine Kopie der Quelldatei mit dem Namen des festen Links, die in das Backup verschoben wurde. Verknüpfungen mit den anderen harten Links zur Quelldatei werden nicht wiederhergestellt.

Schadsoftware-Untersuchung.

Schadsoftware-Untersuchung – Eine auf Befehl ausgeführte, einmalige vollständige oder benutzerdefinierte Untersuchung der Dateien auf einem Gerät. Kaspersky Endpoint Security kann mehrere Aufgaben zur Schadsoftware-Untersuchung gleichzeitig ausführen.

Die Anwendung erstellt eine vordefinierte Aufgabe vom Typ *Schadsoftware-Untersuchung (Scan_My_Computer)*. Mit dieser Aufgabe können Sie eine vollständige Untersuchung des Geräts durchführen. Bei der vollständigen Untersuchung untersucht die 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.

Wenn ein Benutzer mit root-Berechtigung keinen Zugriff auf eine Datei in einem über NFSv4 eingebundenen Remote-Verzeichnis hat, blockiert die Anwendung den Zugriff auf die Datei für alle Benutzer.

In Kaspersky Security Center erstellt der Assistent für die Erstkonfiguration von Kaspersky Security Center nach der Installation des MMC-Plug-ins oder des Web-Plug-ins für die Verwaltung von Kaspersky Endpoint Security automatisch eine Gruppenaufgabe zur Schadsoftware-Untersuchung.

Während der vollständigen Festplattenuntersuchung wird die CPU ausgelastet sein. Es wird empfohlen, die vollständige Festplattenuntersuchung durchzuführen, wenn sich das System im Ruhezustand befindet.

Sie können Einstellungen für automatisch erstellte Aufgaben in Kaspersky Security Center und über die Befehlszeile konfigurieren sowie Benutzeraufgaben zur Schadsoftware-Untersuchung erstellen.

Wenn Schadsoftware entdeckt wird, kann Kaspersky Endpoint Security die infizierte Datei löschen und den von dieser Datei gestarteten schädlichen Prozess beenden.

Wenn die Anwendung während Schadsoftware-Untersuchung von einem Kontrolldienst oder vom Benutzer manuell neu gestartet wurde, wird die Aufgabenausführung unterbrochen. Die Anwendung protokolliert dann das Ereignis *OnDemandTaskInterrupted*.

Sie können Aufgaben zur Schadsoftware-Untersuchung starten und Untersuchungseinstellungen konfigurieren:

- Wählen Sie Betriebssystemobjekte aus, die untersucht werden müssen: Dateien, Archive, Bootsektoren, Prozess- und Kernelspeicher sowie Autostart-Objekte.
- Begrenzen Sie die Größe des untersuchten Objekts und die Untersuchungsdauer für das Objekt.
- Wählen Sie die Aktionen aus, welche die Anwendung für infizierte Objekte ausführen soll.
- Konfigurieren Sie den Ausschluss von Objekten von der Untersuchung nach:
  - Namen oder Masken
  - Namen der in den Objekten gefundenen Bedrohungen

Bei Betriebssystemen mit speziellem parsecfs-Dateisystem (Astra Linux Special Edition) wird es empfohlen, die Mount-Pfade dieses Dateisystems zu den Untersuchungsausnahmen hinzuzufügen.

- Aktivieren oder deaktivieren der Verwendung von globalen Ausnahmen und von Ausnahmen aus dem Schutz vor bedrohlichen Dateien während der Untersuchung.
- Aktivieren Sie die Protokollierung von Informationen zu untersuchten nicht infizierten Objekten, zu untersuchten Objekten in Archiven und zu nicht verarbeiteten Objekten.
- Konfigurieren Sie die Verwendung der heuristischen Analyse und der iChecker-Technologie während der Untersuchung.
- Beschränken Sie die Anzahl der Geräte, deren Bootsektoren untersucht werden müssen.
- Konfigurieren Sie Untersuchungsbereiche und von der Untersuchung auszuschließende Bereiche.

Schadsoftware-Untersuchung in der Web Console

In der Web Console können Sie mithilfe der Aufgabe *Schadsoftware-Untersuchung* nach Schadsoftware suchen.

Sie können eine automatisch erstellte Gruppenaufgabe starten sowie Benutzeraufgaben für die Untersuchung erstellen und starten. Sie können die Untersuchungseinstellungen anpassen, indem Sie die Einstellungen der Aufgaben zur Schadsoftware-Untersuchung ändern.

Untersuchungsparameter der Aufgabe zur Schadsoftware-Untersuchung

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 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)** konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Archive. Dieses Kontrollkästchen ist standardmäßig aktiviert.
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 das Kontrollkästchen aktiviert ist, untersucht die Anwendung selbstentpackende Archive. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung 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 mit 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 Anwendung 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.

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 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 die Anwendung nur neue oder seit der letzten Untersuchung geänderte Dateien. 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 die Ebene der heuristischen Analyse in der Dropdown-Liste festlegen: • **Oberflächlich** – Die am wenigsten detaillierte Untersuchung, minimale Systembelastung. • **Mittel** – Mittlere Untersuchung, ausgeglichene Systembelastung. • **Tief** – Detaillierteste Untersuchung, maximale Systembelastung. • **Empfohlen** (Standardwert) – Optimale Stufe, die von den Kaspersky-Experten empfohlen wird. Sie bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Geräte.
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.
Untersuchungsbereiche	Eine Tabelle mit Bereichen, die von der Aufgabe untersucht werden sollen. Standardmäßig enthält die Tabelle einen Untersuchungsbereich, der alle Verzeichnisse des lokalen Dateisystems umfasst. Sie können Untersuchungsbereiche in der Tabelle hinzufügen, ändern, löschen, nach oben verschieben und nach unten verschieben. Sie können auch eine Liste mit Untersuchungsbereichen aus einer Datei importieren, indem Sie auf die Schaltfläche **Importieren** klicken und die Liste der Untersuchungsbereiche über die Schaltflächen **Exportieren** in eine Datei im JSON-Format exportieren. Beim Importieren wird Ihnen vorgeschlagen, entweder die Liste der Untersuchungsbereiche zu ersetzen oder die Untersuchungsbereiche zu einer bestehenden Liste hinzuzufügen.

Fenster zum Hinzufügen des Untersuchungsbereichs

In diesem Fenster können Sie einen neuen Untersuchungsbereich hinzufügen oder anpassen.

Einstellungen des Untersuchungsbereichs

Parameter	Description
Name des Bereichs	Eingabefeld für den Namen der Untersuchungsbereichs. Dieser Name wird in der Tabelle **Untersuchungsbereiche** im Abschnitt **Untersuchungseinstellungen** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung dieses Bereichs während der Ausführung der 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	In der Dropdown-Liste können Sie den Typ des Dateisystems auswählen: • **Lokal** (Standardwert) – Lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie den Pfad zu einem lokalen Verzeichnis angeben. • **Mounted** – Gemountete Remote-Verzeichnisse oder lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie das Protokoll oder den Namen des Dateisystems angeben. • **Freigegeben** – Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind. • **Alle freigegebenen** – Alle Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind.
Zugriffsprotokoll	In der Dropdown-Liste können Sie das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind. Diese Dropdown-Liste ist verfügbar, wenn in der Dropdown-Liste für Dateisysteme als Typ **Freigegeben** oder **Mounted** ausgewählt ist.

Parameter	Description
Path	Eingabefeld für den Pfad des Verzeichnisses, das in den Untersuchungsbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie **Masken** und **Tags** verwenden. Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben: • `[container-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` Wobei gilt: `<ID>` ist die Container-ID. `<Name>` ist ein Containername `<Pfad zum lokalen Verzeichnis>` 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>]/Pfad zum lokalen Verzeichnis>`. Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert. Beispiel: • `[container-name:<Name>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` • `[container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>][image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][image-id:<ID>][container-id:<ID>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardmäßige Pfadangabe **/** – Die Anwendung untersucht alle Verzeichnisse des lokalen Dateisystems. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Lokal** ausgewählt ist. Wenn in der Dropdown-Liste der Dateisysteme als Typ **Lokal** ausgewählt ist und kein Pfad angegeben wird, untersucht die Anwendung alle Verzeichnisse des lokalen Dateisystems.
Name der freigegebenen Ressource	Eingabefeld für den Namen der freigegebenen Ressource des Dateisystems, auf der sich die Verzeichnisse befinden, die Sie zum Untersuchungsbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste **Zugriffsprotokoll** das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der Anwendung während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske ***** (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen.

Abschnitt "Untersuchungsbereiche"

Sie können die Einstellungen für den Untersuchungsbereich der Aufgabe zur Schadsoftware-Untersuchung anpassen. Die Anwendung ermöglicht die Untersuchung von Dateien, Bootsektoren, und Speicher des Client-Geräts, sowie von Autostart-Objekten.

Parameter für den Untersuchungsbereich der Aufgabe zur Schadsoftware-Untersuchung

Parameter	Description
Dateien untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Dateien. Wenn das Kontrollkästchen aktiviert ist, untersucht die Anwendung Dateien. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Dateien. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Bootsektoren untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Bootsektoren. Wenn das Kontrollkästchen aktiviert ist, untersucht die Anwendung 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 Client-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 die Anwendung Autostart-Objekte. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Autostart-Objekte. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Zu untersuchende Geräte	Der Link **Gerätemasken** anpassen öffnet das Fenster **Untersuchungsbereiche**. In diesem Fenster können Sie die Geräte angeben, deren Bootsektoren untersucht werden sollen.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält die Masken der Gerätenamen, deren Bootsektoren die Anwendung untersuchen soll. Standardmäßig enthält die Tabelle die Gerätenamen-Maske **/**** (alle Geräte).

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Abschnitt "Ausschlussbereiche"

Im Abschnitt **Ausschlussbereiche** der Aufgabe "Schadsoftware-Untersuchung" können Sie die Ausschlussbereiche, die Ausschlüsse nach Maske und Bedrohungsname sowie die Verwendung globaler Ausschlüsse und Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der Ausführung der Aufgabe konfigurieren.

Einstellungen der Ausnahmen von der Untersuchung

Parameter	Description
Ausschlussbereich anpassen	Der Link **Ausschlussbereiche anpassen** öffnet das Fenster **Ausschlussbereiche**. In diesem Fenster können Sie eine Liste mit Ausschlüsse von der Untersuchung festlegen.
Ausschlüsse nach Maske anpassen	Der Link **Ausschlüsse nach Maske konfigurieren** öffnet das Fenster **Ausschlüsse nach Maske**. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren.
Ausschlüsse nach Bedrohungsname anpassen	Der Link **Ausschlüsse nach Bedrohungsname konfigurieren** öffnet das Fenster **Ausschlüsse nach Bedrohungsname**. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren.
Globale Ausnahmen verwenden	Das Kontrollkästchen aktiviert oder deaktiviert den Ausschluss von in den globalen Ausnahmen angegeben Mountpunkten während der 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 "Ausschlussbereiche"

Das Fenster enthält die Ausschlussbereiche einer Untersuchung. Die Anwendung untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden.

Einstellungen des Ausschlussbereichs

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 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 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.

Fenster zum Hinzufügen des Ausschlussbereichs

In diesem Fenster können Sie einen neuen Ausschlussbereich 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 während der Ausführung der Anwendung. Wenn das Kontrollkästchen aktiviert ist, wird dieser Bereich während der Ausführung der Anwendung von der Untersuchung oder vom Schutz ausgeschlossen. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich während der Ausführung der Anwendung in die Untersuchung oder den Schutz eingeschlossen. Im Folgenden können Sie diesen Bereich von der Untersuchung oder dem Schutz ausschließen, indem Sie das Kontrollkästchen aktivieren. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	In der Dropdown-Liste können Sie den Typ des Dateisystems auswählen, auf dem sich die Verzeichnisse befinden, die Sie zu den Ausschlüssen von der Untersuchung hinzufügen möchten: • **Lokal** – Lokale Verzeichnisse. • **Mounted** – Remote-Verzeichnisse, die auf dem Gerät eingebunden sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind.
Zugriffsprotokoll	In der Dropdown-Liste können Sie das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind. Diese Dropdown-Liste ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** ausgewählt ist.

Parameter	Description
Path	Eingabefeld für den Pfad des Verzeichnisses, das in den Ausschlussbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie **Masken** und **Tags** verwenden. Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben: • `[container-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` Wobei gilt: `<ID>` ist die Container-ID. `<Name>` ist ein Containername `<Pfad zum lokalen Verzeichnis>` 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>]/Pfad zum lokalen Verzeichnis>`. Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert. Beispiel: • `[container-name:<Name>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` • `[container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>][image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][image-id:<ID>][container-id:<ID>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Als Pfad ist standardmäßig **/** angegeben. Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Lokal** ausgewählt ist.
Name der freigegebenen Ressource	Eingabefeld für den Namen der freigegebenen Ressource des Dateisystems, auf der sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten: Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste **Zugriffsprotokoll** das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der Anwendung von der Untersuchung ausgeschlossen werden. Die Masken werden nur innerhalb des Verzeichnisses übernommen, das im Eingabefeld **Pfad** angegeben ist. Standardmäßig enthält die Liste die Maske ***** (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen.

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** oder **Ändern** 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 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.

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.

Ein Klick auf die Schaltfläche **Hinzufügen** oder **Ändern** öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung angeben, die von der Untersuchung ausgenommen wird.

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.

Schadsoftware-Untersuchung in der Verwaltungskonsole

In der Verwaltungskonsole können Sie mithilfe der Aufgabe *Schadsoftware-Untersuchung* nach Schadsoftware suchen.

Sie können eine automatisch erstellte Gruppenaufgabe starten sowie Benutzeraufgaben für die Untersuchung erstellen und starten. Sie können die Untersuchungseinstellungen anpassen, indem Sie die Einstellungen der Aufgaben zur Schadsoftware-Untersuchung ändern.

Im Abschnitt **Einstellungen** in den Eigenschaften der Aufgabe "Schadsoftware-Untersuchung" können Sie die in der folgenden Tabelle aufgeführten Einstellungen konfigurieren.

Untersuchungsparameter der Aufgabe zur Schadsoftware-Untersuchung

Parameter	Description
Untersuchung	Diese Einstellungsgruppe enthält Schaltflächen, mit denen Fenster geöffnet werden können, in denen Sie die Untersuchungsbereiche, die Einstellungen des Untersuchungsbereichs und die Untersuchungseinstellungen anpassen können.
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.

Im Abschnitt **Ausnahmen** in den Einstellungen der Aufgabe zur Schadsoftware-Untersuchung können Sie Ausschlussbereiche, Ausschlüsse nach Maske und Ausschlüsse nach Bedrohungsname konfigurieren.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält den Untersuchungsbereich. Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle einen Untersuchungsbereich, der alle Verzeichnisse des lokalen Dateisystems umfasst.

Einstellungen des Untersuchungsbereichs

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 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 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.

Parameter	Description
	Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Untersuchungsbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie **Masken** und **Tags** verwenden. Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben: • `[container-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` Wobei gilt: `<ID>` ist die Container-ID. `<Name>` ist ein Containername `<Pfad zum lokalen Verzeichnis>` 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>]/Pfad zum lokalen Verzeichnis>`. Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert. Beispiel: • `[container-name:<Name>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` • `[container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>][image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][image-id:<ID>][container-id:<ID>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardmäßige Pfadangabe **/** – Die 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.

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 die Anwendung Dateien. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Dateien. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Bootsektoren untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Bootsektoren. Wenn das Kontrollkästchen aktiviert ist, untersucht die Anwendung 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 die Anwendung 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 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)** konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Archive. Dieses Kontrollkästchen ist standardmäßig aktiviert.
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 das Kontrollkästchen aktiviert ist, untersucht die Anwendung selbstentpackende Archive. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung 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 mit 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 Anwendung 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.

Parameter	Description
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 die Anwendung nur neue oder seit der letzten Untersuchung geänderte Dateien. 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 die Ebene der heuristischen Analyse in der Dropdown-Liste festlegen: • **Oberflächlich** – Die am wenigsten detaillierte Untersuchung, minimale Systembelastung. • **Mittel** – Mittlere Untersuchung, ausgeglichene Systembelastung. • **Tief** – Detaillierteste Untersuchung, maximale Systembelastung. • **Empfohlen** (Standardwert) – Optimale Stufe, die von den Kaspersky-Experten empfohlen wird. Sie bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Geräte.

Fenster "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 Anwendung untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden.

Einstellungen des Ausschlussbereichs

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 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.

Parameter	Description
	Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Ausschlussbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie **Masken** und **Tags** verwenden. Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben: • `[container-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` Wobei gilt: `<ID>` ist die Container-ID. `<Name>` ist ein Containername `<Pfad zum lokalen Verzeichnis>` 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>]/Pfad zum lokalen Verzeichnis>`. Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert. Beispiel: • `[container-name:<Name>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` • `[container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>][image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][image-id:<ID>][container-id:<ID>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Als Pfad ist standardmäßig **/** angegeben. Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus.
Name des Dateisystems	Eingabefeld für den Namen des Dateisystems, auf dem sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste auf der rechten Seite das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der 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.

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).

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.

Schadsoftware-Untersuchung über die Befehlszeile

Über die Befehlszeile können Sie auf folgende Arten eine Schadsoftware-Untersuchung durchführen:

- Mithilfe der vordefinierten Aufgabe "Schadsoftware-Untersuchung" (*Scan_My_Computer*). Sie können diese Aufgabe manuell starten, beenden, anhalten und fortsetzen und den Zeitplan für den Aufgabenstart konfigurieren. Sie können die Einstellungen für die Untersuchung konfigurieren, indem Sie die Einstellungen für diese Aufgabe ändern.

- Mithilfe von Benutzeraufgaben zur Schadsoftware-Untersuchung (Aufgaben vom Typ *ODS*). Sie können Benutzeraufgaben manuell starten, beenden, anhalten und fortsetzen und den Zeitplan für den Aufgabenstart konfigurieren.

Mit dem Befehl `kesl-control --scan-file` können Sie eine *benutzerdefinierte Untersuchung* der angegebenen Dateien und Verzeichnisse durchführen.

Einstellungen der vordefinierten Aufgabe zur Schadsoftware-Untersuchung

Die Tabelle beschreibt alle möglichen Werte sowie die Standardwerte aller Einstellungen, die Sie für die Aufgabe „Schadsoftware-Untersuchung“ angeben können.

Untersuchungsparameter der Aufgabe zur Schadsoftware-Untersuchung

Parameter	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) – Prozess-Speicher und Kernelspeicher untersuchen. `No` – Prozess-Speicher 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 Anwendungsdatenbanken 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.

Parameter	Description	Werte
`ScanPlainMail`	Aktiviert die Untersuchung von E-Mail-Nachrichten im Textformat (plain text).	`Yes` – E-Mail-Nachrichten im Textformat 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 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: 0.
`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, aus der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht aus 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 den Wert dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseExcludeMasks` aktiviert ist.
		Der Standardwert ist nicht angegeben.
		Beispiel:
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Ermöglicht es, für Objekte, die die durch die Einstellung `ExcludeThreats.item_#` festgelegten Bedrohungen enthalten, Ausnahmen von Untersuchungen zu erstellen.	`Ja` — Objekte, die 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.

Parameter	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 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`

`UseGlobalExclusions`	Aktivieren der Verwendung von globalen Ausnahmen während der Untersuchung.	`Yes` (Standardwert) – Globale Ausnahmen verwenden. `No` – Keine globale Ausnahmen verwenden.
`UseOASExclusions`	Aktivieren der Verwendung der Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der Untersuchung.	`Yes` (Standardwert) – Ausschlüsse aus dem Schutz vor bedrohlichen Dateien verwenden. `No` – Keine Ausschlüsse aus dem Schutz vor bedrohlichen Dateien verwenden.
`ReportCleanObjects`	Aktiviert die Protokollierung von Informationen zu untersuchten Objekten, welche die Anwendung 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 die Untersuchung von Objekten, die zu einem Archiv gehören, im Protokoll speichern. `No` (Standardwert) – Informationen über die Untersuchung von Objekten, die zu einem Archiv gehören, nicht im Protokoll speichern.
`ReportUnprocessedObjects`	Aktiviert das Protokollieren von Informationen über Objekte, die aus einem bestimmten Grund nicht verarbeitet wurden.	`Yes` – Informationen zu nicht verarbeiteten Objekten im Protokoll speichern. `No` (Standardwert) – Informationen zu nicht verarbeiteten Objekten nicht im Protokoll speichern.
`UseAnalyzer`	Aktiviert die heuristische Analyse. 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.

Parameter	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` – Mittlere Ebene der heuristischen Analyse mit ausgeglichener Belastung des Betriebssystems. `Deep` – Gründlichste Untersuchung mit maximaler Belastung des Betriebssystems. `Recommended` (Standardwert) – Der empfohlene Wert.
`UseIChecker`	Aktiviert die Nutzung der iChecker-Technologie.	`Yes` (Standardwert) – Nutzung der iChecker-Technologie aktivieren. `No` – Nutzung der iChecker-Technologie deaktivieren.
`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. `< Maske für Gerätenamen >` – Bootsektoren der Geräte untersuchen, deren Namen mit der angegebenen Maske übereinstimmen. Standardwert: `/**` (beliebiger Zeichensatz im Gerätenamen, einschließlich des Zeichens `/`)
Der Abschnitt **[ScanScope.item_#]** enthält die folgenden Parameter:		
`AreaDesc`	Beschreibung des Untersuchungsbereichs, der erweiterte Informationen über den Untersuchungsbereich enthält. Die maximale Länge einer Zeichenfolge, die mit dieser Einstellung angegeben werden kann, beträgt 4096 Zeichen.	Standardwert: `All objects` Beispiel: `AreaDesc=" Mail bases scan "`
`UseScanArea`	Aktiviert die Untersuchung des angegebenen Bereichs. Um die Aufgabe auszuführen, müssen Sie mindestens einen zu untersuchenden Bereich angeben.	`Yes` (Standardwert) – Den angegebenen Bereich untersuchen. `No` – Angegebenen Bereich nicht untersuchen.
`AreaMask.item_#`	Einschränkung des Untersuchungsbereichs. Im Untersuchungsbereich untersucht die 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_< Nummer des Elements >=*doc`
`Path`	Pfad zum Verzeichnis mit untersuchten Objekten.	`< Pfad zum lokalen Verzeichnis >` — Objekte im angegebenen Verzeichnis untersuchen. `Shared:NFS` – Ressourcen des Gerätedateisystems untersuchen, auf die über das NFS-Protokoll zugegriffen wird. `Shared:SMB` – Ressourcen des Gerätedateisystems untersuchen, auf die über das Samba-Protokoll zugegriffen wird. `Mounted:NFS` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über NFS-Protokoll eingebunden sind. `Mounted:SMB` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über das Samba-Protokoll eingebunden sind. `AllRemoteMounted` – alle Remote-Verzeichnisse untersuchen, die auf dem Gerät über Samba- oder NFS-Protokolle gemountet sind. `AllShared` – Ressourcen des Gerätedateisystems untersuchen, auf die über das Samba- und NFS-Protokoll zugegriffen wird. `<Dateisystemtyp>` – Alle Ressourcen des angegebenen Dateisystemgeräts untersuchen.
Der Abschnitt **[ExcludedFromScanScope.item_#]** enthält die folgenden Parameter:		

Parameter	Description	Werte
`AreaDesc`	Beschreibung des Ausschlussbereichs, der erweiterte Informationen über den Ausschlussbereich enthält.	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 Anwendung alle Objekte im Ausschlussbereich aus. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: `*` (alle Objekte ausschließen)
`Path`	Pfad zum Verzeichnis mit ausgeschlossenen Objekten.	`<Pfad zum lokalen Verzeichnis>` – Objekte im angegebenen Verzeichnis (einschließlich Unterverzeichnissen) von Untersuchungen ausschließen. Bei der Angabe des Pfades können Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Bei Systemen mit dem Dateisystem BTRFS und aktivierten aktiven Snapshots wird es zur Optimierung der Untersuchungsaufgaben empfohlen, den Pfad mit dem im "Read only"-Modus gemounteten Snapshots den Ausschlüssen hinzuzufügen. Beispielsweise können in Systemen auf Basis von SUSE/OpenSUSE eines Ausschluss folgendermaßen angeben: `/.snapshots/*/snapshot/`. Als 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. `<Dateisystemtyp>` – 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.

Benutzerdefinierte Untersuchung von Dateien und Verzeichnissen über die Befehlszeile

Sie können eine benutzerdefinierte Untersuchung der angegebenen Dateien und Verzeichnisse mithilfe des folgenden Befehls durchführen: `kesl-control --scan-file`.

Eine benutzerdefinierte Untersuchung wird mit den Einstellungen durchgeführt, die in der vordefinierten Aufgabe *Scan_File* (ID:3) gespeichert sind. Sie können die Einstellungen für die benutzerdefinierte Dateiuntersuchung konfigurieren, indem Sie die Einstellungen dieser Aufgabe ändern (siehe Tabelle unten).

Um eine benutzerdefinierte Untersuchung der angegebenen Dateien und Verzeichnisse durchzuführen, führen Sie den folgenden Befehl aus:

```
kesl-control --scan-file <Pfad> [--action <Aktion>]
```

wobei:

- `<Pfad>` – Pfad zu der Datei oder dem Verzeichnis, das Sie überprüfen möchten. Sie können mehrere, durch Leerzeichen getrennte Pfade angeben.
- `--action <Aktion>` – Aktion, welche die Anwendung für infizierte Objekte ausführen soll. Mögliche Werte: `DisinfectDeleteIfNotPossible, DisinfectInformIfNotPossible, Inform`. Wenn Sie den Schalter `--action` nicht angeben, führt die Anwendung die Aktion `DisinfectDeleteIfNotPossible` aus.

Als Ergebnis der Ausführung des Befehls wird eine temporäre Aufgabe zur Untersuchung von Dateien erstellt, die nach Abschluss automatisch gelöscht wird. Gleichzeitig werden die Ergebnisse der Untersuchung in die Konsole ausgegeben.

Die Tabelle beschreibt alle möglichen Werte sowie die Standardwerte aller Einstellungen, die Sie für die Aufgabe *Scan_File* angeben können.

Die in der Aufgabe `Scan_File` angegebenen Abschnitte `[ScanScope.item_#]` und *[ExcludedFromScanScope.item_#]* werden bei der Durchführung einer benutzerdefinierten Untersuchung nicht berücksichtigt.

Einstellungen der Aufgabe Scan_File

Parameter	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.

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.	`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 Textformat 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 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: 0.
`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, aus der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht aus 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.*`

Parameter	Description	Werte
`UseExcludeThreats`	Ermöglicht es, für Objekte, die die durch die Einstellung `ExcludeThreats.item_#` festgelegten Bedrohungen enthalten, Ausnahmen von Untersuchungen zu erstellen.	`Ja` — Objekte, die 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`

`UseGlobalExclusions`	Aktivieren der Verwendung von globalen Ausnahmen während der Untersuchung.	`Yes` (Standardwert) – Globale Ausnahmen verwenden. `No` – Keine globale Ausnahmen verwenden.
`UseOASExclusions`	Aktivieren der Verwendung der Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der Untersuchung.	`Yes` (Standardwert) – Ausschlüsse aus dem Schutz vor bedrohlichen Dateien verwenden. `No` – Keine Ausschlüsse aus dem Schutz vor bedrohlichen Dateien verwenden.
`ReportCleanObjects`	Aktiviert die Protokollierung von Informationen zu untersuchten Objekten, welche die Anwendung 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 die Untersuchung von Objekten, die zu einem Archiv gehören, im Protokoll speichern. `No` (Standardwert) – Informationen über die Untersuchung von Objekten, die zu einem Archiv gehören, nicht im Protokoll speichern.
`ReportUnprocessedObjects`	Aktiviert das Protokollieren von Informationen über Objekte, die aus einem bestimmten Grund nicht verarbeitet wurden.	`Yes` – Informationen zu nicht verarbeiteten Objekten im Protokoll speichern. `No` (Standardwert) – Informationen zu nicht verarbeiteten Objekten nicht im Protokoll speichern.
`UseAnalyzer`	Aktiviert die heuristische Analyse. 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.

Parameter	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` – Mittlere Ebene der heuristischen Analyse mit ausgeglichener Belastung des Betriebssystems. `Deep` – Gründlichste Untersuchung mit maximaler Belastung des Betriebssystems. `Recommended` (Standardwert) – Der empfohlene Wert.
`UseIChecker`	Aktiviert die Nutzung der iChecker-Technologie.	`Yes` (Standardwert) – Nutzung der iChecker-Technologie aktivieren. `No` – Nutzung der iChecker-Technologie deaktivieren.
`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. `< Maske für Gerätenamen >` – Bootsektoren der Geräte untersuchen, deren Namen mit der angegebenen Maske übereinstimmen. Standardwert: `/**` (beliebiger Zeichensatz im Gerätenamen, einschließlich des Zeichens `/`)
Der Abschnitt **[ScanScope.item_#]** enthält die folgenden Parameter:		
`AreaDesc`	Beschreibung des Untersuchungsbereichs, der erweiterte Informationen über den Untersuchungsbereich enthält. Die maximale Länge einer Zeichenfolge, die mit dieser Einstellung angegeben werden kann, beträgt 4096 Zeichen.	Standardwert: `All objects` Beispiel: `AreaDesc=" Mail-Datenbanken untersuchen "`
`UseScanArea`	Aktiviert die Untersuchung des angegebenen Bereichs. Um die Aufgabe auszuführen, müssen Sie mindestens einen zu untersuchenden Bereich angeben.	`Yes` (Standardwert) – Den angegebenen Bereich untersuchen. `No` – Angegebenen Bereich nicht untersuchen.
`AreaMask.item_#`	Einschränkung des Untersuchungsbereichs. Im Untersuchungsbereich untersucht die 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_< Nummer des Elements >=*doc`
`Path`	Pfad zum Verzeichnis mit untersuchten Objekten.	`< Pfad zum lokalen Verzeichnis >` — Objekte im angegebenen Verzeichnis untersuchen. `Shared:NFS` – Ressourcen des Gerätedateisystems untersuchen, auf die über das NFS-Protokoll zugegriffen wird. `Shared:SMB` – Ressourcen des Gerätedateisystems untersuchen, auf die über das Samba-Protokoll zugegriffen wird. `Mounted:NFS` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über NFS-Protokoll eingebunden sind. `Mounted:SMB` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über das Samba-Protokoll eingebunden sind. `AllRemoteMounted` – alle Remote-Verzeichnisse untersuchen, die auf dem Gerät über Samba- oder NFS-Protokolle gemountet sind. `AllShared` – Ressourcen des Gerätedateisystems untersuchen, auf die über das Samba- und NFS-Protokoll zugegriffen wird. `<Dateisystemtyp>` – Alle Ressourcen des angegebenen Dateisystemgeräts untersuchen.
Der Abschnitt **[ExcludedFromScanScope.item_#]** enthält die folgenden Parameter:		

Parameter	Description	Werte
`AreaDesc`	Beschreibung des Ausschlussbereichs, der erweiterte Informationen über den Ausschlussbereich enthält.	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 Anwendung alle Objekte im Ausschlussbereich aus. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: `*` (alle Objekte ausschließen)
`Path`	Pfad zum Verzeichnis mit ausgeschlossenen Objekten.	`<Pfad zum lokalen Verzeichnis>` – Objekte im angegebenen Verzeichnis (einschließlich Unterverzeichnissen) von Untersuchungen ausschließen. Bei der Angabe des Pfades können Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Bei Systemen mit dem Dateisystem BTRFS und aktivierten aktiven Snapshots wird es zur Optimierung der Untersuchungsaufgaben empfohlen, den Pfad mit dem im "Read only"-Modus gemounteten Snapshots den Ausschlüssen hinzuzufügen. Beispielsweise können in Systemen auf Basis von SUSE/OpenSUSE eines Ausschluss folgendermaßen angeben: `/.snapshots/*/snapshot/`. Als 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. `<Dateisystemtyp>` – 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.

Untersuchung wichtiger Bereiche.

Während der Untersuchung wichtiger Bereiche kann Kaspersky Endpoint Security Bootsektoren, Autostart-Objekte, Prozess- und Kernelspeicher untersuchen.

Wenn Schadsoftware entdeckt wird, kann die App die infizierte Datei löschen und den von dieser Datei gestarteten schädlichen Prozess beenden.

Wenn ein Benutzer mit root-Berechtigung keinen Zugriff auf eine Datei in einem über NFSv4 eingebundenen Remote-Verzeichnis hat, blockiert die Anwendung den Zugriff auf die Datei für alle Benutzer.

So können Sie eine Untersuchung wichtiger Bereiche durchführen und Untersuchungseinstellungen konfigurieren:

- Wählen Sie die zu untersuchenden Betriebssystemobjekte aus. Standardmäßig ist die Untersuchung von Bootsektoren, Prozess- und Kernelspeicher, Autostart-Objekten und Archiven aktiviert. Bei der Untersuchung wichtiger Bereiche werden Dateien standardmäßig nicht untersucht.
- Begrenzen Sie die Größe des untersuchten Objekts und die Untersuchungsdauer für das Objekt.
- Wählen Sie die Aktionen aus, welche die Anwendung für infizierte Objekte ausführen soll.
- Konfigurieren Sie den Ausschluss von Objekten von der Untersuchung nach:
  - Namen oder Masken
  - Namen der in den Objekten gefundenen Bedrohungen

  Bei Betriebssystemen mit speziellem parsecfs-Dateisystem (Astra Linux Special Edition) wird es empfohlen, die Mount-Pfade dieses Dateisystems zu den Untersuchungsausnahmen hinzuzufügen.
- Aktivieren oder deaktivieren der Verwendung von globalen Ausnahmen und von Ausnahmen aus dem Schutz vor bedrohlichen Dateien während der Untersuchung.
- Aktivieren Sie die Protokollierung von Informationen zu untersuchten nicht infizierten Objekten, zu untersuchten Objekten in Archiven und zu nicht verarbeiteten Objekten.
- Konfigurieren Sie die Verwendung der heuristischen Analyse und der iChecker-Technologie während der Untersuchung.
- Beschränken Sie die Anzahl der Geräte, deren Bootsektoren untersucht werden müssen.
- Konfigurieren Sie Untersuchungsbereiche und von der Untersuchung auszuschließende Bereiche.

Untersuchung wichtiger Bereiche in der Web Console

In der Web Console können Sie mithilfe der Aufgabe *Untersuchung wichtiger Bereiche* wichtige Bereiche des Betriebssystems des geschützten Geräts untersuchen.

Sie können Benutzeraufgaben zur Untersuchung wichtiger Bereiche erstellen und starten. Sie können die Untersuchungseinstellungen konfigurieren, indem Sie die Aufgabeneinstellungen ändern.

Einstellungen der Aufgabe zur Untersuchung wichtiger Bereiche

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 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)** konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Archive. Dieses Kontrollkästchen ist standardmäßig aktiviert.
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 das Kontrollkästchen aktiviert ist, untersucht die Anwendung selbstentpackende Archive. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung 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 mit 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 Anwendung 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.
Über nicht verarbeitete Dateien informieren	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 die Anwendung nur neue oder seit der letzten Untersuchung geänderte Dateien. 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 die Ebene der heuristischen Analyse in der Dropdown-Liste festlegen: • **Oberflächlich** – Die am wenigsten detaillierte Untersuchung, minimale Systembelastung. • **Mittel** – Mittlere Untersuchung, ausgeglichene Systembelastung. • **Tief** – Detaillierteste Untersuchung, maximale Systembelastung. • **Empfohlen** (Standardwert) – Optimale Stufe, die von den Kaspersky-Experten empfohlen wird. Sie bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Geräte.
Aktion beim Fund einer Bedrohung	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.
Untersuchungsbereiche	Eine Tabelle mit Bereichen, die von der Aufgabe untersucht werden sollen. Standardmäßig enthält die Tabelle einen Untersuchungsbereich, der alle Verzeichnisse des lokalen Dateisystems umfasst. Sie können Untersuchungsbereiche in der Tabelle hinzufügen, ändern, löschen, nach oben verschieben und nach unten verschieben. Sie können auch eine Liste mit Untersuchungsbereichen aus einer Datei importieren, indem Sie auf die Schaltfläche **Importieren** klicken und die Liste der Untersuchungsbereiche über die Schaltflächen **Exportieren** in eine Datei im JSON-Format exportieren. Beim Importieren wird Ihnen vorgeschlagen, entweder die Liste der Untersuchungsbereiche zu ersetzen oder die Untersuchungsbereiche zu einer bestehenden Liste hinzuzufügen.

Fenster zum Hinzufügen des Untersuchungsbereichs

In diesem Fenster können Sie einen neuen Untersuchungsbereich hinzufügen oder anpassen.

Einstellungen des Untersuchungsbereichs

Parameter	Description
Name des Bereichs	Eingabefeld für den Namen der Untersuchungsbereichs. Dieser Name wird in der Tabelle **Untersuchungsbereiche** im Abschnitt **Untersuchungseinstellungen** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung dieses Bereichs während der Ausführung der 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	In der Dropdown-Liste können Sie den Typ des Dateisystems auswählen: • **Lokal** (Standardwert) – Lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie den Pfad zu einem lokalen Verzeichnis angeben. • **Mounted** – Gemountete Remote-Verzeichnisse oder lokale Verzeichnisse. Wenn dieses Element ausgewählt ist, müssen Sie das Protokoll oder den Namen des Dateisystems angeben. • **Freigegeben** – Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind. • **Alle freigegebenen** – Alle Dateisystemressourcen geschützter Server, die über das Samba- oder NFS-Protokoll zugänglich sind.
Zugriffsprotokoll	In der Dropdown-Liste können Sie das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind. Diese Dropdown-Liste ist verfügbar, wenn in der Dropdown-Liste für Dateisysteme als Typ **Freigegeben** oder **Mounted** ausgewählt ist.

Parameter	Description
Path	Eingabefeld für den Pfad des Verzeichnisses, das in den Untersuchungsbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie **Masken** und **Tags** verwenden. Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben: • `[container-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` Wobei gilt: `<ID>` ist die Container-ID. `<Name>` ist ein Containername `<Pfad zum lokalen Verzeichnis>` 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>]/Pfad zum lokalen Verzeichnis>`. Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert. Beispiel: • `[container-name:<Name>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` • `[container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>][image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][image-id:<ID>][container-id:<ID>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardmäßige Pfadangabe **/** – Die Anwendung untersucht alle Verzeichnisse des lokalen Dateisystems. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Lokal** ausgewählt ist. Wenn in der Dropdown-Liste der Dateisysteme als Typ **Lokal** ausgewählt ist und kein Pfad angegeben wird, untersucht die Anwendung alle Verzeichnisse des lokalen Dateisystems.
Name der freigegebenen Ressource	Eingabefeld für den Namen der freigegebenen Ressource des Dateisystems, auf der sich die Verzeichnisse befinden, die Sie zum Untersuchungsbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste **Zugriffsprotokoll** das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der Anwendung während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske ***** (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen.

Abschnitt "Untersuchungsbereiche"

Einstellungen des Untersuchungsbereichs der Aufgabe zur Untersuchung wichtiger Bereiche

Parameter	Description
Dateien untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Dateien. Wenn das Kontrollkästchen aktiviert ist, untersucht die Anwendung Dateien. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Dateien. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Bootsektoren untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Bootsektoren. Wenn das Kontrollkästchen aktiviert ist, untersucht die Anwendung Bootsektoren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Bootsektoren. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Kernel-Speicher und gestartete Prozesse untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung des Arbeitsspeichers des Client-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 aktiviert.
Autostart-Objekte untersuchen	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung von Autostart-Objekten. Wenn das Kontrollkästchen aktiviert ist, untersucht die Anwendung Autostart-Objekte. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Autostart-Objekte. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Zu untersuchende Geräte	Der Link **Gerätemasken** anpassen öffnet das Fenster **Untersuchungsbereiche**. In diesem Fenster können Sie die Geräte angeben, deren Bootsektoren untersucht werden sollen.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält die Masken der Gerätenamen, deren Bootsektoren die Anwendung untersuchen soll. Standardmäßig enthält die Tabelle die Gerätenamen-Maske **/**** (alle Geräte).

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

Abschnitt "Ausschlussbereiche"

Im Abschnitt **Ausschlussbereiche** der Aufgabe "Untersuchung wichtiger Bereiche" können Sie die Ausschlussbereiche, die Ausschlüsse nach Maske und Bedrohungsname sowie die Verwendung globaler Ausschlüsse und Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der Ausführung der Aufgabe konfigurieren.

Einstellungen der Ausnahmen von der Untersuchung

Parameter	Description
Ausschlussbereich anpassen	Der Link **Ausschlussbereiche anpassen** öffnet das Fenster **Ausschlussbereiche**. In diesem Fenster können Sie eine Liste mit Ausschlüsse von der Untersuchung festlegen.
Ausschlüsse nach Maske anpassen	Der Link **Ausschlüsse nach Maske konfigurieren** öffnet das Fenster **Ausschlüsse nach Maske**. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren.

Parameter	Description
Ausschlüsse nach Bedrohungsname anpassen	Der Link **Ausschlüsse nach Bedrohungsname konfigurieren** öffnet das Fenster **Ausschlüsse nach Bedrohungsname**. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren.
Globale Ausnahmen verwenden	Das Kontrollkästchen aktiviert oder deaktiviert den Ausschluss von in den globalen Ausnahmen angegeben Mountpunkten während der 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 "Ausschlussbereiche"

Das Fenster enthält die Ausschlussbereiche einer Untersuchung. Die Anwendung untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden.

Einstellungen des Ausschlussbereichs

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 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 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.

Fenster zum Hinzufügen des Ausschlussbereichs

In diesem Fenster können Sie einen neuen Ausschlussbereich 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 während der Ausführung der Anwendung. Wenn das Kontrollkästchen aktiviert ist, wird dieser Bereich während der Ausführung der Anwendung von der Untersuchung oder vom Schutz ausgeschlossen. Wenn das Kontrollkästchen deaktiviert ist, wird dieser Bereich während der Ausführung der Anwendung in die Untersuchung oder den Schutz eingeschlossen. Im Folgenden können Sie diesen Bereich von der Untersuchung oder dem Schutz ausschließen, indem Sie das Kontrollkästchen aktivieren. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Dateisystem, Zugriffsprotokoll und Pfad	In der Dropdown-Liste können Sie den Typ des Dateisystems auswählen, auf dem sich die Verzeichnisse befinden, die Sie zu den Ausschlüssen von der Untersuchung hinzufügen möchten: • **Lokal** – Lokale Verzeichnisse. • **Mounted** – Remote-Verzeichnisse, die auf dem Gerät eingebunden sind. • **Alle remote-mounted** – Alle Remote-Verzeichnisse, die auf dem Gerät über die Samba- und NFS-Protokolle eingebunden sind.
Zugriffsprotokoll	In der Dropdown-Liste können Sie das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind. • **Benutzerdefiniert** – Ressourcen des Dateisystems des Geräts, die im nachfolgenden Feld angegeben sind. Diese Dropdown-Liste ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** ausgewählt ist.

Parameter	Description
Path	Eingabefeld für den Pfad des Verzeichnisses, das in den Ausschlussbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie **Masken** und **Tags** verwenden. Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben: • `[container-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` Wobei gilt: `<ID>` ist die Container-ID. `<Name>` ist ein Containername `<Pfad zum lokalen Verzeichnis>` 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>]/Pfad zum lokalen Verzeichnis>`. Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert. Beispiel: • `[container-name:<Name>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` • `[container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>][image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][image-id:<ID>][container-id:<ID>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Als Pfad ist standardmäßig **/** angegeben. Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Lokal** ausgewählt ist.
Name der freigegebenen Ressource	Eingabefeld für den Namen der freigegebenen Ressource des Dateisystems, auf der sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten: Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste **Zugriffsprotokoll** das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der Anwendung von der Untersuchung ausgeschlossen werden. Die Masken werden nur innerhalb des Verzeichnisses übernommen, das im Eingabefeld **Pfad** angegeben ist. Standardmäßig enthält die Liste die Maske ***** (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen.

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** oder **Ändern** 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 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.

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.

Ein Klick auf die Schaltfläche **Hinzufügen** oder **Ändern** öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung angeben, die von der Untersuchung ausgenommen wird.

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.

Untersuchung wichtiger Bereiche in der Verwaltungskonsole

In der Verwaltungskonsole können Sie mithilfe der Aufgabe *Untersuchung wichtiger Bereiche* wichtige Bereiche des Betriebssystems des geschützten Geräts untersuchen.

Sie können Benutzeraufgaben zur Untersuchung wichtiger Bereiche erstellen und starten. Sie können die Untersuchungseinstellungen konfigurieren, indem Sie die Aufgabeneinstellungen ändern.

Im Abschnitt **Einstellungen** in den Eigenschaften der Aufgabe "Untersuchung wichtiger Bereiche" können Sie die in der folgenden Tabelle aufgeführten Einstellungen konfigurieren.

Einstellungen der Aufgabe zur Untersuchung wichtiger Bereiche

Parameter	Description
Untersuchung	Diese Einstellungsgruppe enthält Schaltflächen, mit denen Fenster geöffnet werden können, in denen Sie die Untersuchungsbereiche, die Einstellungen des Untersuchungsbereichs und die Untersuchungseinstellungen anpassen können.
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.

Im Abschnitt **Ausnahmen** in den Einstellungen der Aufgabe zur Untersuchung wichtiger Bereiche können Sie Ausschlussbereiche, Ausschlüsse nach Maske und Ausschlüsse nach Bedrohungsname konfigurieren.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält den Untersuchungsbereich. Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle einen Untersuchungsbereich, der alle Verzeichnisse des lokalen Dateisystems umfasst.

Einstellungen des Untersuchungsbereichs

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 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 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.

Parameter	Description
	Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Untersuchungsbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie **Masken** und **Tags** verwenden. Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben: • `[container-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` Wobei gilt: `<ID>` ist die Container-ID. `<Name>` ist ein Containername `<Pfad zum lokalen Verzeichnis>` 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>]/Pfad zum lokalen Verzeichnis>`. Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert. Beispiel: • `[container-name:<Name>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` • `[container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>][image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][image-id:<ID>][container-id:<ID>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardmäßige Pfadangabe **/** – Die 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.

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.

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 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)** konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Archive. Dieses Kontrollkästchen ist standardmäßig aktiviert.
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 das Kontrollkästchen aktiviert ist, untersucht die Anwendung selbstentpackende Archive. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung 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 mit 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 Anwendung 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.

Parameter	Description
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 die Anwendung nur neue oder seit der letzten Untersuchung geänderte Dateien. 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 die Ebene der heuristischen Analyse in der Dropdown-Liste festlegen: • **Oberflächlich** – Die am wenigsten detaillierte Untersuchung, minimale Systembelastung. • **Mittel** – Mittlere Untersuchung, ausgeglichene Systembelastung. • **Tief** – Detaillierteste Untersuchung, maximale Systembelastung. • **Empfohlen** (Standardwert) – Optimale Stufe, die von den Kaspersky-Experten empfohlen wird. Sie bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Geräte.

Fenster "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 Anwendung untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden.

Einstellungen des Ausschlussbereichs

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 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.

Parameter	Description
	Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Ausschlussbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie **Masken** und **Tags** verwenden. Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben: • `[container-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` Wobei gilt: `<ID>` ist die Container-ID. `<Name>` ist ein Containername `<Pfad zum lokalen Verzeichnis>` 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>]/Pfad zum lokalen Verzeichnis>`. Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert. Beispiel: • `[container-name:<Name>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` • `[container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>][image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][image-id:<ID>][container-id:<ID>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Als Pfad ist standardmäßig **/** angegeben. Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus.
Name des Dateisystems	Eingabefeld für den Namen des Dateisystems, auf dem sich die Verzeichnisse befinden, die Sie zum Ausschlussbereich hinzufügen möchten. Das Feld ist verfügbar, wenn in der Dropdown-Liste mit Dateisystemen als Typ **Mounted** und in der Dropdown-Liste auf der rechten Seite das Element **Benutzerdefiniert** ausgewählt sind.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der 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.

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).

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.

Untersuchung wichtiger Bereiche über die Befehlszeile

Über die Befehlszeile können Sie mithilfe der vordefinierten Aufgabe zur Untersuchung wichtiger Bereiche (*Critical_Areas_Scan*) wichtige Bereiche des Betriebssystems des geschützten Geräts untersuchen.

Sie können diese Aufgabe manuell starten, beenden, anhalten und fortsetzen und den Zeitplan für den Aufgabenstart konfigurieren. Sie können Untersuchungseinstellungen konfigurieren, indem Sie die Einstellungen für diese Aufgabe ändern.

Parameter	Description	Werte
`ScanFiles`	Aktiviert die Untersuchung von Dateien.	`Yes` – Dateien untersuchen. `Nein` (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.	`Ja` (Standardwert) — Prozessspeicher und Kernelspeicher untersuchen. `No` – Prozess-Speicher 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 Anwendungsdatenbanken 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 Textformat 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 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: 0.
`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`.

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, aus der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht aus 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 den Wert dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseExcludeMasks` aktiviert ist.
		Der Standardwert ist nicht angegeben.
		Beispiel:
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Ermöglicht es, für Objekte, die die durch die Einstellung `ExcludeThreats.item_#` festgelegten Bedrohungen enthalten, Ausnahmen von Untersuchungen zu erstellen.	`Ja` — Objekte, die 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`

`UseGlobalExclusions`	Aktivieren der Verwendung von globalen Ausnahmen während der Untersuchung.	`Yes` (Standardwert) – Globale Ausnahmen verwenden. `No` – Keine globale Ausnahmen verwenden.
`UseOASExclusions`	Aktivieren der Verwendung der Ausschlüsse aus dem Schutz vor bedrohlichen Dateien während der Untersuchung.	`Yes` (Standardwert) – Ausschlüsse aus dem Schutz vor bedrohlichen Dateien verwenden. `No` – Keine Ausschlüsse aus dem Schutz vor bedrohlichen Dateien verwenden.
`ReportCleanObjects`	Aktiviert die Protokollierung von Informationen zu untersuchten Objekten, welche die Anwendung 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.

Parameter	Description	Werte
`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 die Untersuchung von Objekten, die zu einem Archiv gehören, im Protokoll speichern. `No` (Standardwert) – Informationen über die Untersuchung von Objekten, die zu einem Archiv gehören, nicht im Protokoll speichern.
`ReportUnprocessedObjects`	Aktiviert das Protokollieren von Informationen über Objekte, die aus einem bestimmten Grund nicht verarbeitet wurden.	`Yes` – Informationen zu nicht verarbeiteten Objekten im Protokoll speichern. `No` (Standardwert) – Informationen zu nicht verarbeiteten Objekten nicht im Protokoll speichern.
`UseAnalyzer`	Aktiviert die heuristische Analyse. 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` – Mittlere Ebene der heuristischen Analyse mit ausgeglichener Belastung des Betriebssystems. `Deep` – Gründlichste Untersuchung mit maximaler Belastung des Betriebssystems. `Recommended` (Standardwert) – Der empfohlene Wert.
`UseIChecker`	Aktiviert die Nutzung der iChecker-Technologie.	`Yes` (Standardwert) – Nutzung der iChecker-Technologie aktivieren. `No` – Nutzung der iChecker-Technologie deaktivieren.
`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. `< Maske für Gerätenamen >` – Untersuchung der Bootsektoren von den Geräten, deren Namen von der Maske eingeschlossen werden. Standardwert: `/**` (beliebiger Zeichensatz im Gerätenamen, einschließlich des Zeichens `/`)
Der Abschnitt **[ScanScope.item_#]** enthält die folgenden Parameter:		
`AreaDesc`	Beschreibung des Untersuchungsbereichs, der erweiterte Informationen über den Untersuchungsbereich enthält. Die maximale Länge einer Zeichenfolge, die mit dieser Einstellung angegeben werden kann, beträgt 4096 Zeichen.	Standardwert: `All objects` Beispiel: `AreaDesc=" Mail bases scan "`
`UseScanArea`	Aktiviert die Untersuchung des angegebenen Bereichs. Um die Aufgabe auszuführen, müssen Sie mindestens einen zu untersuchenden Bereich angeben.	`Yes` (Standardwert) – Den angegebenen Bereich untersuchen. `No` – Angegebenen Bereich nicht untersuchen.
`AreaMask.item_#`	Einschränkung des Untersuchungsbereichs. Im Untersuchungsbereich untersucht die 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_< Nummer des Elements >=*doc`

Parameter	Description	Werte
`Path`	Pfad zum Verzeichnis mit untersuchten Objekten.	`< Pfad zum lokalen Verzeichnis >` — Objekte im angegebenen Verzeichnis untersuchen. `Shared:NFS` – Ressourcen des Gerätedateisystems untersuchen, auf die über das NFS-Protokoll zugegriffen wird. `Shared:SMB` – Ressourcen des Gerätedateisystems untersuchen, auf die über das Samba-Protokoll zugegriffen wird. `Mounted:NFS` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über NFS-Protokoll eingebunden sind. `Mounted:SMB` – Remote-Verzeichnisse untersuchen, die auf dem Gerät über das Samba-Protokoll eingebunden sind. `AllRemoteMounted` – alle Remote-Verzeichnisse untersuchen, die auf dem Gerät über Samba- oder NFS-Protokolle gemountet sind. `AllShared` – Ressourcen des Gerätedateisystems untersuchen, auf die über das Samba- und NFS-Protokoll zugegriffen wird. `<Dateisystemtyp>` – Alle Ressourcen des angegebenen Dateisystemgeräts untersuchen.
Der Abschnitt **[ExcludedFromScanScope.item_#]** enthält die folgenden Parameter:		
`AreaDesc`	Beschreibung des Ausschlussbereichs, der erweiterte Informationen über den Ausschlussbereich enthält.	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 Anwendung alle Objekte im Ausschlussbereich aus. Sie können für diese Einstellung mehrere Werte angeben.	Standardwert: `*` (alle Objekte ausschließen)

Parameter	Description	Werte
`Path`	Pfad zum Verzeichnis mit ausgeschlossenen Objekten.	`<Pfad zum lokalen Verzeichnis>` – Objekte im angegebenen Verzeichnis (einschließlich Unterverzeichnissen) von Untersuchungen ausschließen. Bei der Angabe des Pfades können Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Bei Systemen mit dem Dateisystem BTRFS und aktivierten aktiven Snapshots wird es zur Optimierung der Untersuchungsaufgaben empfohlen, den Pfad mit dem im "Read only"-Modus gemounteten Snapshots den Ausschlüssen hinzuzufügen. Beispielsweise können in Systemen auf Basis von SUSE/OpenSUSE eines Ausschluss folgendermaßen angeben: `/.snapshots/*/snapshot/`. Als 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. `<Dateisystemtyp>` – 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.

Untersuchung von Wechseldatenträgern

Kaspersky Endpoint Security kann die folgenden Wechseldatenträger bei Anschluss an das geschützte Gerät untersuchen: CD-/DVD-Laufwerke, Blu-ray-Discs, Flash-Laufwerke (einschließlich USB-Modems), externe Festplatten und Disketten.

Wenn die Untersuchung von Wechseldatenträgern aktiviert ist, überwacht Kaspersky Endpoint Security die Verbindung von Wechseldatenträgern mit dem geschützten Gerät und untersucht, wenn ein angeschlossener Wechseldatenträger erkannt wird, das Laufwerk und seine Bootsektoren auf Viren und andere Malware.

Standardmäßig kontrolliert die Anwendung den Anschluss von Wechseldatenträgern nicht und untersucht sie auch nicht.

Untersuchung von Wechseldatenträgern in der Web Console konfigurieren

In der Web Console können Sie Einstellungen zur Untersuchung von Wechseldatenträgern in den Richtlinieneigenschaften konfigurieren (**Anwendungseinstellungen** → **Host-Schutz** → **Untersuchung von Wechseldatenträgern**).

Untersuchung von Wechseldatenträgern in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen für die Untersuchung von Wechseldatenträgern in den Richtlinieneigenschaften verwalten (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**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. 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. • **Genaue Untersuchung** – Dient zur Untersuchung aller Dateien auf Wechseldatenträgern (außer CD/DVD-Laufwerken und Blu-ray-Discs). Die genaue Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Schadsoftware-Untersuchung* durchgeführt.

Parameter	Description
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. 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. • **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.

Untersuchung von Wechseldatenträgern über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Untersuchung von Wechseldatenträgern mithilfe der vordefinierten Aufgabe *Untersuchung von Wechseldatenträgern* (*Removable_Drives_Scan*) verwalten.

Die Aufgabe *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 Typ *ODS*). 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 CD-/DVD-Laufwerken und Blu-ray-Discs) untersuchen. Die detaillierte Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Scan_File* (ID:3) durchgeführt. `QuickScan` – Es werden nur Dateien **bestimmter Typen** auf Wechseldatenträgern (außer CD-/DVD-Laufwerken und Blu-ray-Discs) untersucht. Auf Wechseldatenträgern werden die folgenden Dateiformate überprüft: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, 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.
`ScanOpticalDrives`	Aktiviert die Untersuchung von CD-/DVD-Laufwerken und Blu-ray-Discs, sobald diese an das Gerät angeschlossen werden.	`DetailedScan` – Alle Dateien auf CD-/DVD-Laufwerken und Blu-ray-Discs untersuchen. Die detaillierte Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Scan_File* (ID:3) durchgeführt. `QuickScan` – Untersucht nur Dateien **bestimmter Typen** auf CD-/DVD-Laufwerken und Blu-ray-Discs. Auf Wechseldatenträgern werden die folgenden Dateiformate überprüft: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. Die schnelle Untersuchung wird mit den Standardeinstellungen für die Aufgabe *Critical_Areas_Scan* (ID:4) durchgeführt. `NoScan` (Standardwert) – Beim Anschluss von CD-/DVD-Laufwerken und Blu-ray-Discs keine Untersuchung ausführen
`BlockDuringScan`	Aktivierung der Blockierung von Dateien auf dem angeschlossenen Datenträger während der Untersuchung. Während der Untersuchung von Bootsektoren werden Dateien nicht blockiert.	`Yes` – Dateien während der Untersuchung blockieren. `No` (Standardwert) – Dateien während der Untersuchung nicht blockieren.

Container untersuchen

Sie können die Untersuchung von Containern und Images auf Schadsoftware in Echtzeit und auf Befehl durchführen:

- Die *Komponente „Container-Überwachung“ (Untersuchung von Containern, Container-Überwachung)* ermöglicht die Untersuchung von Containern beim Start sowie von Namespaces in Echtzeit.
- Mithilfe von Aufgaben vom Typ *Untersuchung von Containern* können Sie Container und Images auf Befehl untersuchen.

Um die Funktion zur Untersuchung von Containern nutzen zu können, benötigen Sie eine Lizenz, in der diese Funktion enthalten ist.

Das Programm unterstützt die Integration in das Container-Management-System Docker, in die CRI-O-Umgebung sowie in die Dienstprogramme Podman und runc.

Es wird die Integration mit dem System zur Verwaltung von Docker-Containern der Version 28.5.2 und niedriger unterstützt.

Container-Überwachung

Standardmäßig ist die Komponente "Container-Überwachung" aktiviert. Die Anwendung untersucht gestartete Container und Namespaces in Echtzeit.

Damit die Komponente "Container-Überwachung" funktioniert, muss die Komponente Schutz vor bedrohlichen Dateien aktiviert sein. Bei der Untersuchung von Containern und Namensräumen werden die Einstellungen des Schutzes vor bedrohlichen Dateien verwendet.

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 für die Container-Überwachung über die Befehlszeile als `Aufgabe ist verfügbar und wird nicht ausgeführt` angezeigt, während er in Kaspersky Security Center als "`Beendet`" angezeigt wird.

Sie können die Komponente "Container-Überwachung" aktivieren oder deaktivieren sowie die Einstellungen der Untersuchung von Containern und Namensräume in Echtzeit konfigurieren:

- Sie können eine Aktion auswählen, die von der Anwendung beim Fund eines infizierten Objekts für den Container ausgeführt werden soll.

  Dieser Parameter ist verfügbar, wenn die Anwendung im Rahmen einer Lizenz verwendet wird, von der diese Funktion abgedeckt wird.

- Sie können die Integration von Kaspersky Endpoint Security mit dem System zur Verwaltung von Docker-Containern, der CRI-O-Umgebung und den Tools Podman und runc konfigurieren.

  Es wird die Integration mit dem System zur Verwaltung von Docker-Containern der Version 28.5.2 und niedriger unterstützt.

Container-Überwachung in der Web Console konfigurieren

In der Web Console können Sie in den Richtlinieneigenschaften (**Programmeinstellungen → Allgemeine Einstellungen → Einstellungen der Untersuchung von Containern**) die Komponente Einstellungen für die Untersuchung von Containern verwalten.

Container-Überwachung in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Richtlinie mithilfe der Verwaltungskonsole erstellen) (**Allgemeine Einstellungen → Einstellungen für die Untersuchung von Containern**) die Einstellungen der Programmablaufverfolgung verwalten.

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.

Parameter	Description
Docker verwenden	Dieses Kontrollkästchen aktiviert oder deaktiviert die Verwendung des Systems zur Verwaltung von Docker-Containern. Dieses Kontrollkästchen ist standardmäßig aktiviert. Es wird die Verwendung des Systems zur Verwaltung von Docker-Containern der Version 28.5.2 und niedriger unterstützt.
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
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-Überwachung über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Echtzeitüberwachung von Namespaces und Containern mit der Option `NamespaceMonitoring=Yes/No` in den Allgemeinen Anwendungseinstellungen aktivieren oder deaktivieren.

Sie können den Wert der Einstellung `NamespaceMonitoring` mithilfe der Konfigurationsdatei, die alle allgemeinen Anwendungseinstellungen enthält, oder mithilfe von Befehlszeilenschaltern ändern.

Für die Echtzeituntersuchung von Namespaces und Containern werden die allgemeinen Einstellungen der Untersuchung von Containern verwendet. Sie können diese Einstellungen mithilfe spezieller Verwaltungsbefehle für Kaspersky Endpoint Security anzeigen und ändern:

- Sie können die aktuellen Werte der allgemeinen Einstellungen für die Untersuchung von Containern in die Konsole oder in eine Konfigurationsdatei ausgeben. Diese Datei können Sie verwenden, um Parameter zu ändern.
- Sie können alle allgemeinen Einstellungen der 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 `< Einstellungsname >= < Einstellungswert >` bearbeiten. Mit dem Befehl zur Ausgabe der allgemeinen Einstellungen für die Untersuchung von Containern können Sie die aktuellen Werte der Einstellungen abrufen.

Um die aktuellen Werte der allgemeinen Einstellungen für die Untersuchung von Containern in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-container-settings [--json]
```

wobei `--json` angegeben wird, 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 allgemeinen Einstellungen für die Untersuchung von Containern in eine Datei auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --get-container-settings --file <Pfad der Konfigurationsdatei> [--json]
```

wobei:

- `--file <Pfad der Konfigurationsdatei>` – Pfad der Konfigurationsdatei, in der die allgemeinen Einstellungen der Untersuchung von Containern 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` wird angegeben, um die Einstellungen im JSON-Format auszugeben. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

So ändern Sie die Werte der allgemeinen Einstellungen für die Untersuchung von Containern mithilfe einer Konfigurationsdatei:

1. Geben Sie die allgemeinen Einstellungen der 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 Befehl aus:

   ```
   kesl-control --set-container-settings --file <Pfad der Konfigurationsdatei> [--json]
   ```

   wobei:

   - `--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei mit den allgemeinen Einstellungen für die Untersuchung von Containern.
   - Geben Sie die Option `--json` an, wenn Sie Einstellungen aus einer JSON-Konfigurationsdatei 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 für die Untersuchung von Containern werden in die Anwendung importiert.

Um die Werte der allgemeinen Einstellungen für die Untersuchung von Containern mithilfe von Befehlszeilenschaltern zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-container-settings <Name der Einstellung>=<Wert der Einstellung>
[<Name der Einstellung>=<Wert der Einstellung>]
```

Wobei gilt: `<Name der Einstellung>=<Wert der Einstellung>` – Name und Wert einer der allgemeinen Einstellungen für die Untersuchung von Containern.

Die Werte der angegebenen allgemeinen Einstellungen für die Untersuchung von Containern werden geändert.

Untersuchung von Containern und Images auf Befehl

Während die Aufgabe zur *Untersuchung von Containern* ausgeführt wird, untersucht Kaspersky Endpoint Security Container und Images auf Viren und andere Malware. Die Anwendung kann mehrere Aufgaben zur Untersuchung von Containern gleichzeitig ausführen.

Um die Aufgabe zur Untersuchung von Containern nutzen zu können, benötigen Sie eine Lizenz, in der diese Funktion enthalten ist.

Das Programm unterstützt die Integration in das Container-Management-System Docker, in die CRI-O-Umgebung sowie in die Dienstprogramme Podman und runc.

Es wird die Integration mit dem System zur Verwaltung von Docker-Containern der Version 28.5.2 und niedriger unterstützt.

So können Sie die Untersuchung von Containern starten und Untersuchungseinstellungen konfigurieren:

- Geben Sie die zu untersuchenden Container und Bilder nach Name oder Namensmaske an.
- Starten Sie die Untersuchung aller Ebenen von Images und Containern.
- Wählen Sie die Aktion aus, welche die Anwendung für den Container ausführen soll, und die Aktion, welche die Anwendung für das Image ausführen soll, wenn ein infiziertes Objekt erkannt wird.
- Konfigurieren Sie die Einstellungen zur Untersuchung von Objekten in Containern oder Images:
  - Aktivieren und deaktivieren Sie die Untersuchung von Archiven, E-Mail-Datenbanken und E-Mail-Nachrichten im Textformat.
  - Begrenzen Sie die Größe des untersuchten Objekts und die Untersuchungsdauer für das Objekt.
  - Wählen Sie die Aktionen aus, welche die Anwendung für infizierte Objekte ausführen soll.
  - Konfigurieren Sie den Ausschluss von Objekten von der Untersuchung nach:
    - Namen oder Masken
    - Namen der in den Objekten gefundenen Bedrohungen
  - Aktivieren oder deaktivieren der Verwendung globaler Ausnahmen bei der Untersuchung.

- Konfigurieren Sie die Verwendung der heuristischen Analyse und der iChecker-Technologie während der Untersuchung.

- Aktivieren und deaktivieren Sie die Protokollierung von Informationen zu untersuchten nicht infizierten Objekten, zu untersuchten Objekten in Archiven und zu nicht verarbeiteten Objekten.

Untersuchung von Containern in der Web Console

In der Web Console können Sie Container und Images mithilfe der Aufgabe *Untersuchung von Containern* untersuchen.

Sie können Benutzeraufgaben für die Untersuchung von Containern erstellen und starten. Sie können die Untersuchungseinstellungen konfigurieren, indem Sie die Aufgabeneinstellungen ändern.

Einstellungen der Aufgabe zur Untersuchung von Containern

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 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)** konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Archive. Dieses Kontrollkästchen ist standardmäßig aktiviert.
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 das Kontrollkästchen aktiviert ist, untersucht die Anwendung selbstentpackende Archive. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung 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 mit 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 Anwendung 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.

Parameter	Description
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 die Anwendung nur neue oder seit der letzten Untersuchung geänderte Dateien. 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 die Ebene der heuristischen Analyse in der Dropdown-Liste festlegen: • **Oberflächlich** – Die am wenigsten detaillierte Untersuchung, minimale Systembelastung. • **Mittel** – Mittlere Untersuchung, ausgeglichene Systembelastung. • **Tief** – Detaillierteste Untersuchung, maximale Systembelastung. • **Empfohlen** (Standardwert) – Optimale Stufe, die von den Kaspersky-Experten empfohlen wird. Sie bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Geräte.
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.
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).
Aktion beim Fund einer Bedrohung	Sie können eine Aktion auswählen, die von der Anwendung beim Fund eines infizierten Objekts für das Image ausgeführt werden soll: • **Container überspringen** und keine Aktion für den Container ausführen, wenn ein infiziertes Objekt erkannt wird. • **Container anhalten** – Hält den Container an, wenn ein infiziertes Objekt erkannt wird. • **Anhalten, falls Desinfektion fehlschlägt** (Standardwert) – Hält den Container an, wenn die Desinfektion eines infizierten Objekts fehlgeschlagen ist oder die Bedrohung nicht beseitigt werden konnte. Aufgrund von Besonderheiten der Funktionsweise von CRI-O-Umgebungen werden infizierte Objekte in den Containern einer CRI-O-Umgebung weder desinfiziert noch gelöscht. Es wird empfohlen, den Vorgang **Container anhalten** auszuwählen.

Parameter	Description
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	Sie können 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.

Abschnitt "Ausschlussbereiche"

Im Abschnitt **Ausschlussbereiche** der Aufgabe "Untersuchung von Containern" können Sie die Ausschlüsse nach Maske und nach Bedrohungsnamen sowie die Verwendung globaler Ausnahmen während der Aufgabenausführung konfigurieren.

Einstellungen der Ausnahmen von der Untersuchung

Parameter	Description
Ausschlüsse nach Maske anpassen	Der Link **Ausschlüsse nach Maske konfigurieren** öffnet das Fenster **Ausschlüsse nach Maske**. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand einer Namensmaske konfigurieren.
Ausschlüsse nach Bedrohungsname anpassen	Der Link **Ausschlüsse nach Bedrohungsname konfigurieren** öffnet das Fenster **Ausschlüsse nach Bedrohungsname**. In diesem Fenster können Sie den Ausschluss von Objekten aus der Untersuchung anhand des Namens einer Bedrohung konfigurieren.
Globale Ausnahmen verwenden	Das Kontrollkästchen aktiviert oder deaktiviert den Ausschluss von in den globalen Ausnahmen angegeben Mountpunkten während der 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** oder **Ändern** 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 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.

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.

Ein Klick auf die Schaltfläche **Hinzufügen** oder **Ändern** öffnet das Fenster **Bedrohungsname**. In diesem Fenster können Sie den Namen der Bedrohung angeben, die von der Untersuchung ausgenommen wird.

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.

Untersuchung von Containern in der Verwaltungskonsole

In der Verwaltungskonsole können Sie Container und Images mithilfe der Aufgabe *Untersuchung von Containern* untersuchen.

Sie können Benutzeraufgaben für die Untersuchung von Containern erstellen und starten. Sie können die Untersuchungseinstellungen konfigurieren, indem Sie die Aufgabeneinstellungen ändern.

Im Abschnitt **Einstellungen** in den Eigenschaften der Aufgabe "Untersuchung von Containern" können Sie die in der folgenden Tabelle aufgeführten Einstellungen konfigurieren.

Einstellungen der Aufgabe zur Untersuchung von Containern

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.

Im Abschnitt **Ausschlüsse** können Sie in den Eigenschaften der Aufgabe zur Untersuchung von Containern auch Ausschlüsse Nach Maske und Nach Bedrohungsname konfigurieren.

Fenster "Einstellungen der Container-Untersuchung"

In diesem Fenster können Sie die Einstellungen für die Untersuchung von Containern und Images anpassen.

Einstellungen für die Untersuchung von Containern und Images

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).
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 Aktion für den Container ausführen, wenn ein infiziertes Objekt erkannt wird. • **Container anhalten** – Hält den Container an, wenn ein infiziertes Objekt erkannt wird. • **Anhalten, falls Desinfektion fehlschlägt** (Standardwert) – Hält den Container an, wenn die Desinfektion eines infizierten Objekts fehlgeschlagen ist oder die Bedrohung nicht beseitigt werden konnte. Aufgrund von Besonderheiten der Funktionsweise von CRI-O-Umgebungen werden infizierte Objekte in den Containern einer CRI-O-Umgebung weder desinfiziert noch gelöscht. Es wird 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.

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 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)** konfigurieren. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung keine Archive. Dieses Kontrollkästchen ist standardmäßig aktiviert.
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 das Kontrollkästchen aktiviert ist, untersucht die Anwendung selbstentpackende Archive. Wenn das Kontrollkästchen deaktiviert ist, untersucht die Anwendung 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 mit 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 Anwendung 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 die Anwendung nur neue oder seit der letzten Untersuchung geänderte Dateien. 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 die Ebene der heuristischen Analyse in der Dropdown-Liste festlegen: • **Oberflächlich** – Die am wenigsten detaillierte Untersuchung, minimale Systembelastung. • **Mittel** – Mittlere Untersuchung, ausgeglichene Systembelastung. • **Tief** – Detaillierteste Untersuchung, maximale Systembelastung. • **Empfohlen** (Standardwert) – Optimale Stufe, die von den Kaspersky-Experten empfohlen wird. Sie bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Geräte.

Fenster "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).

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.

Untersuchung von Containern über die Befehlszeile

Über die Befehlszeile können Sie die Untersuchung von Containern und Images auf folgende Arten durchführen:

- Mithilfe der vordefinierten Aufgabe Untersuchung von Containern (*Container_Scan*). Sie können diese Aufgabe manuell starten und beenden und den Zeitplan für den Aufgabenstart konfigurieren. Sie können die Einstellungen für die Untersuchung konfigurieren, indem Sie die Einstellungen für diese Aufgabe ändern.
- Mithilfe von Benutzeraufgaben zur Untersuchung von Containern (Aufgaben vom Typ *ContainerScan*). Sie können Benutzeraufgaben manuell starten und beenden und den Zeitplan für den Aufgabenstart konfigurieren.
- Mit dem Befehl `kesl-control --scan-container` können Sie eine *benutzerdefinierte Untersuchung* der angegebenen Container und Images durchführen.

Einstellungen der Aufgabe zur Untersuchung von Containern

Alle verfügbaren Werte und Standardwerte für jede Einstellung der Untersuchung von Containern und Images werden in der nachstehenden Tabelle beschrieben.

Einstellungen der Aufgabe zur Untersuchung von Containern

Parameter	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`	Legt einen Namen oder eine Namensmaske fest, die den zu untersuchenden Container definiert.
	Masken werden im Format der Befehlsschnittstelle angegeben. Sie können die folgenden Symbole verwenden: "?" und "*".
	Bevor Sie diese Einstellung angeben, stellen Sie sicher, dass für die Einstellung der Wert `ScanContainers=Yes` angegeben ist.
		Der Standardwert ist "*" (alle Container untersuchen).
		Beispiele:
		So untersuchen Sie einen Container mit dem Namen my_container:
		`ContainerNameMask=my_container`
		So untersuchen Sie alle Container, deren Namen mit my_container beginnen:
		`ContainerNameMask=my_container*`
		So untersuchen Sie alle Container, deren Namen mit my_ beginnen, dann fünf beliebige Zeichen enthalten und anschließend von _container und einer beliebigen Zeichenfolge gefolgt sind:
		`ContainerNameMask=my_?????_container*`

`ScanImages`	Untersuchung 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.

Parameter	Description	Werte

`ImageNameMask`	Legt einen Namen oder eine Namensmaske fest, welche die zu untersuchenden Images definiert.
	Bevor Sie diese Einstellung festlegen, überzeugen Sie sich, dass der Wert der Einstellung `ScanImages` auf `Yes` festgelegt ist.
	Masken werden im Format der Befehlsschnittstelle angegeben.
	Wenn Sie mehrere Masken angeben möchten, muss jede Maske in einer neuen Zeile mit einem neuen Index angegeben werden.
		Der Standardwert ist "*" (alle Images untersuchen).
		Beispiele:
		So untersuchen Sie ein Image mit dem Namen "my_image" und dem Tag-Wert "latest":
		`ImageNameMask=my_image:latest`
		So untersuchen Sie alle Images, deren Namen mit "my_image_" beginnen und die einen beliebigen Tag-Wert haben:
		`ImageNameMask=my_image*`

`DeepScan`	Untersuchung aller Image-Ebenen und gestarteten Container.	`Yes` – Alle Ebenen untersuchen. `No` (Standardwert) – Nicht alle Ebenen untersuchen.
`ContainerScanAction`	Aktion, die für einen Container ausgeführt werden soll, wenn ein infiziertes Objekt erkannt wird. Die Aktionen für infizierte Objekte in einem Container werden nachfolgend beschrieben.	`StopContainerIfFailed` (Standardwert) – Die 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, die Aktion `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.
`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

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.	`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.

Parameter	Description	Werte
`ScanSfxArchived`	Aktiviert die Untersuchung von nur selbstentpackenden Archiven (Archiven, zu deren Bestandteilen ein ausführbares Dekompressionsmodul gehört).	`Yes` (Standardwert) – Selbstentpackende Archive untersuchen. `No` – Selbstentpackende Archive nicht untersuchen.
`ScanMailBases`	Aktiviert die Untersuchung von E-Mail-Datenbanken von Microsoft Outlook, Outlook Express, The Bat und anderer Mail-Clients.	`Yes` – Dateien von E-Mail-Datenbanken untersuchen. `No` (Standardwert) – Dateien von E-Mail-Datenbanken nicht untersuchen.
`ScanPlainMail`	Aktiviert die Untersuchung von E-Mail-Nachrichten im Textformat (plain text).	`Yes` – E-Mail-Nachrichten im Textformat untersuchen. `No` (Standardwert) – E-Mail-Nachrichten im Textformat nicht untersuchen.
`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: 0.
`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.
`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, aus der Untersuchung ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht aus 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.	`Ja` — Objekte, die 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.

Parameter	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 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`

`UseGlobalExclusions`	Aktivieren der Verwendung von globalen Ausnahmen während der Untersuchung.	`Yes` (Standardwert) – Globale Ausnahmen verwenden. `No` – Keine globale Ausnahmen verwenden.
`ReportCleanObjects`	Aktiviert die Protokollierung von Informationen zu untersuchten Objekten, welche die Anwendung 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 die Untersuchung von Objekten, die zu einem Archiv gehören, im Protokoll speichern. `No` (Standardwert) – Informationen über die Untersuchung von Objekten, die zu einem Archiv gehören, nicht im Protokoll speichern.
`ReportUnprocessedObjects`	Aktiviert das Protokollieren von Informationen über Objekte, die aus einem bestimmten Grund nicht verarbeitet wurden.	`Yes` – Informationen zu nicht verarbeiteten Objekten im Protokoll speichern. `No` (Standardwert) – Informationen zu nicht verarbeiteten Objekten nicht im Protokoll speichern.
`UseAnalyzer`	Aktiviert die heuristische Analyse. 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.

Parameter	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` – Mittlere Ebene der heuristischen Analyse mit ausgeglichener Belastung des Betriebssystems. `Deep` – Gründlichste Untersuchung mit maximaler Belastung des Betriebssystems. `Recommended` (Standardwert) – Der empfohlene Wert.
`UseIChecker`	Aktiviert die Nutzung der iChecker-Technologie.	`Yes` (Standardwert) – Nutzung der iChecker-Technologie aktivieren. `No` – Nutzung der iChecker-Technologie deaktivieren.

Benutzerdefinierte Untersuchung von Containern und Images

Mit dem Befehl `kesl-control --scan-container` können Sie eine benutzerdefinierte Untersuchung der angegebenen Container und Images durchführen.

Eine benutzerdefinierte Untersuchung wird mit Einstellungen durchgeführt, die in der vordefinierten Aufgabe *Custom_Container_Scan* (ID:19) gespeichert sind. Sie können die Einstellungen für die benutzerdefinierte Untersuchung von Containern und Images konfigurieren, indem Sie die Einstellungen für diese Aufgabe ändern. Standardmäßig hat die Aufgabe *Custom_Container_Scan* dieselben Einstellungen wie die Aufgabe *Container_Scan* (ID:18).

Um eine erneute benutzerdefinierte Untersuchung von Containern zu starten, führen Sie den folgenden Befehl aus:

```
kesl-control --scan-container <ID/Name [:Tag]>
```

wobei `<ID/Name [:Tag]>` für den Namen oder die ID des Containers oder Images steht. Um mehrere Objekte zu untersuchen, können Sie **Masken** verwenden.

Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Bei mehreren Entitäten mit demselben Namen untersucht die Anwendung alle Entitäten.

Als Ergebnis der Ausführung des Befehls wird eine temporäre Aufgabe zur Untersuchung von Containern und Images erstellt, die nach Abschluss automatisch gelöscht wird. Gleichzeitig werden die Ergebnisse der Untersuchung in die Konsole ausgegeben.

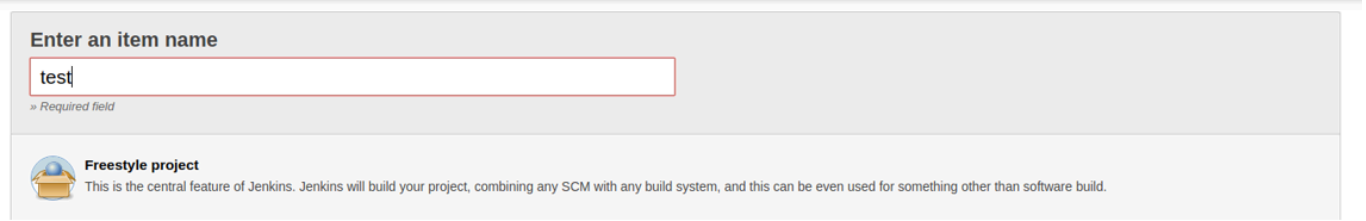
Beispiele:
Untersuchung eines Containers mit dem Namen "my_container":
`kesl-control --scan-container my_container`
Untersucht ein Image namens "my_image" (alle Tags):
`kesl-control --scan-container my_image*`

Integration mit Jenkins

Kaspersky Endpoint Security unterstützt die Integration mit Jenkins. Plug-ins für Jenkins Pipeline können auf verschiedenen Etappen zur Untersuchung von Docker-Images verwendet werden. So können Sie z. B. Docker-Images in einem Repository während des Entwicklungsprozesses oder vor der Veröffentlichung untersuchen.

So integrieren Sie Kaspersky Endpoint Security in Jenkins:

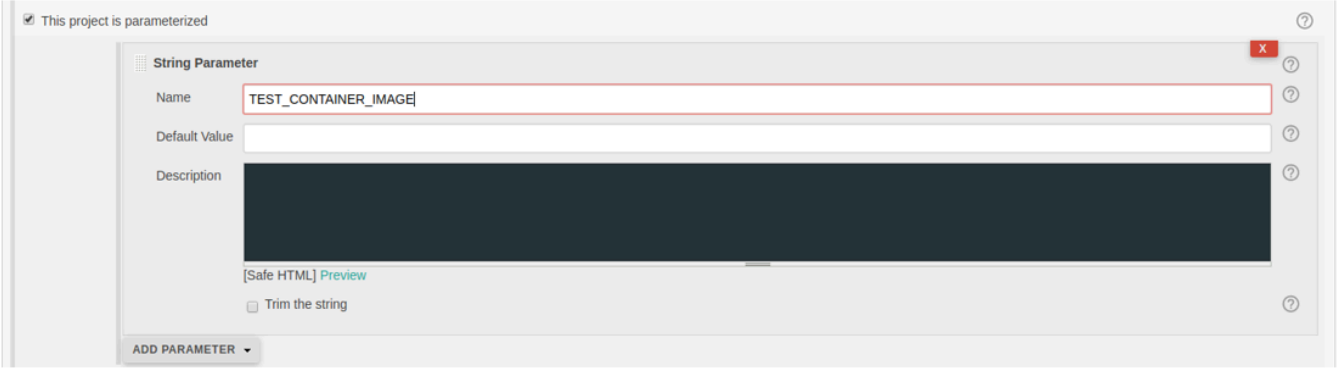
1. Installieren Sie Kaspersky Endpoint Security auf einem Jenkins-Node.
2. Installieren Sie Docker Engine auf einem Jenkins-Node.
   Weitere Informationen finden Sie in der Dokumentation zu Docker Engine.
3. Gewähren Sie dem Nutzer "Jenkins" folgende Administrator-Berechtigungen für Kaspersky Endpoint Security:
   `kesl-control --grant-role admin <Jenkins-Benutzername>`
4. Fügen Sie der Gruppe "docker" einen Jenkins-Benutzer hinzu:
   `sudo usermod -aG docker <Jenkins-Benutzername>`
   Normalerweise wird der Name "jenkins" verwendet.
5. Erstellen Sie in Jenkins eine neue Build-Aufgabe mit dem Namen `test` (**New Item** → **Enter an item name**).



6. Konfigurieren Sie das Projekt nach Ihren Bedürfnissen. Es wird davon ausgegangen, dass Sie in Folge dessen über ein Image oder einen gestarteten Container verfügen, dass Sie untersuchen müssen.
7. Um den Docker-Container zu starten, fügen Sie der Jenkins Build-Prozedur folgendes Skript an. Wenn Sie Jenkins Plug-ins oder andere Werkzeuge verwenden, um Docker-Container zu starten, speichern Sie die ID des ausgeführten Docker-Containers zur weiteren Untersuchung in der Datei /tmp/kesl_cs_info:

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
echo "Start container from image: '${TEST_CONTAINER_IMAGE}'"
CONTAINER_ID=$(docker run -d -v /storage:/storage ${TEST_CONTAINER_IMAGE}
/storage/docker_process.sh)
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot start container from image ${TEST_CONTAINER_IMAGE}"
exit 1
fi
```

```
echo "${CONTAINER_ID}" > ${TMP_FILE}
exit ${EXIT_CODE}
```



8. Nachdem die Artefakte gebaut wurden, fügen Sie den Schritten das folgende Skript hinzu, um Jenkins zu bauen.

   Dieses Skript unterstützt einen zu untersuchenden Container. Bei Bedarf können Sie das Skript Ihren Bedürfnissen anpassen.

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
if [ ! -f "${TMP_FILE}" ] ; then
echo "Cannot find temporary file with container ID: '${TMP_FILE}'"
exit 1
fi
CONTAINER_ID=$(cat ${TMP_FILE})
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot find container ID in the temporary file: '${TMP_FILE}'"
exit 1
fi
echo "Start anti-virus scan for: '${CONTAINER_ID}'"
THREATS_AMOUNT=$(kesl-control --scan-container ${CONTAINER_ID}|grep 'Total detected objects'|awk '{print $5}')
if [ "${THREATS_AMOUNT}" != "0" ] ; then
echo "ATTENTION! ${THREATS_AMOUNT} threats detected at: '${CONTAINER_ID}'"
EXIT_CODE=1
else
echo "Not threats found"
fi
echo "Remove container: {${CONTAINER_ID}}"
docker kill ${CONTAINER_ID}
docker rm -f $CONTAINER_ID
rm -f ${TMP_FILE}
```

9. Verwenden Sie das folgende Skript, um ein Docker-Image aus einem Repository zu untersuchen:

```
DOCKER_FILE=https://raw.githubusercontent.com/ianmiell/simple-dockerfile/master/Dockerfile
```

```
DOCKER_FILE_FETCHED=$$.Dockerfile
TEST_IMAGE_NAME=test_image
echo "Build image from ${DOCKER_FILE}"
curl ${DOCKER_FILE} -o ${DOCKER_FILE_FETCHED}
if [ -f ${DOCKER_FILE_FETCHED} ] ; then
echo "Dockerfile fetched: ${DOCKER_FILE_FETCHED}"
else
echo "Dockerfile not fetched"
exit 1
fi
docker build -f ${DOCKER_FILE_FETCHED} -t ${TEST_IMAGE_NAME}
echo "Scan docker image"
SCAN_RESULT=$(/opt/kaspersky/kesl/bin/kesl-control --scan-container
${TEST_IMAGE_NAME}*)
echo "Scan done: "
echo $SCAN_RESULT
```

10. Speichern Sie den Build-Job.

Firewall-Verwaltung

Bei der Verwendung von lokalen Netzwerken und des Internets ist ein Gerät neben Viren und anderer Schadsoftware auch einer Vielzahl von Angriffen ausgesetzt, die Schwachstellen in Betriebssystemen und Software ausnutzen. Die Firewall des Betriebssystems schützt die auf dem Gerät des Benutzers gespeicherten persönlichen Daten, indem sie die meisten Bedrohungen für das Betriebssystem blockiert, wenn das Gerät mit dem Internet oder einem lokalen Netzwerk verbunden ist.

Mit der Betriebssystem-Firewall können Sie alle Netzwerkverbindungen auf dem Gerät des Benutzers erkennen und eine Liste seiner IP-Adressen bereitstellen. Mit der Komponente "Firewall-Verwaltung" können Sie den Status dieser Netzwerkverbindungen festlegen, indem Sie Netzwerkpaketregeln konfigurieren.

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. Alle ausgehenden Verbindungen werden standardmäßig erlaubt, sofern keine entsprechende Verbotsregeln für die Komponente "Firewall-Verwaltung" angegeben sind.

Standardmäßig ist die Komponente "Firewall-Verwaltung" deaktiviert.

Deaktivieren Sie andere Tools zur Verwaltung der betriebssystemeigenen Firewall, bevor Sie die Komponente „Firewall-Verwaltung“ aktivieren.

Wenn Sie die Komponente "Firewall-Verwaltung" aktivieren, löscht Kaspersky Endpoint Security automatisch alle Benutzerregeln, die für die Firewall mithilfe des Betriebssystems konfiguriert wurden. Nach dem Deaktivieren der Komponente werden diese Regeln nicht wiederhergestellt. Speichern Sie bei Bedarf benutzerdefinierte Firewall-Regeln, bevor Sie die Komponente "Firewall-Verwaltung" aktivieren.

Wenn die Firewall-Verwaltung aktiviert ist, untersucht Kaspersky Endpoint Security die Firewall des Betriebssystems und blockiert jeden Versuch, die Firewall-Einstellungen zu ändern, beispielsweise wenn eine Anwendung oder ein Tool versucht, eine Firewall-Regel hinzuzufügen oder zu entfernen. Kaspersky Endpoint Security überprüft die Firewall des Betriebssystems alle 60 Sekunden und stellt bei Bedarf die mithilfe der Anwendung erstellten Firewall-Regeln wieder her. Das Überprüfungsintervall kann nicht geändert werden.

Kaspersky Endpoint Security überprüft weiterhin die Firewall des Betriebssystems, selbst wenn die Firewall-Verwaltung deaktiviert ist. Das ermöglicht der Anwendung, die dynamischen Regeln wiederherzustellen.

Sie können die Firewall-Verwaltung aktivieren und deaktivieren und auch die folgenden Einstellungen konfigurieren:

- Konfigurieren Sie eine Liste von Netzwerkpaketregeln, die Kaspersky Endpoint Security anwenden soll, wenn es einen Versuch erkennt, eine Netzwerkverbindung herzustellen. Sie können Netzwerkpaketregeln hinzufügen und entfernen sowie die Ausführungspriorität einer Netzwerkpaketregel ändern.

  In einigen Betriebssystemen auf Code-Basis von Red Hat Enterprise Linux können Firewall-Regeln, die mit Kaspersky Endpoint Security erstellt wurden, nur mithilfe von Verwaltungsbefehlen angezeigt werden (Befehl `kesl-control -F --query`).

- Wählen Sie Standardaktionen aus, die mit eingehenden Verbindungen oder Paketen ausgeführt werden sollen, wenn für diese Verbindungsart keine anderen Netzwerkpaketregeln angewendet werden können.

- Legen Sie Netzwerkadressen so fest, dass sie vorinstallierten Netzwerken entsprechen. Sie können IP-Adressen oder Subnetze zu verfügbaren Netzwerken hinzufügen und Adressen aus verfügbaren Netzwerken entfernen.

- Aktivieren und deaktivieren Sie das automatische Hinzufügen von Erlaubnisregeln für Ports des Administrationsagenten.

Über Netzwerkpaketregeln

Netzwerkpaketregeln sind erlaubende oder blockierende Aktionen, die von Kaspersky Endpoint Security ausgeführt werden, wenn eine versuchte Netzwerkverbindung erkannt wird.

Die Regeln legen unabhängig von der Anwendung Beschränkungen für Netzwerkpakete fest. Solche Regeln schränken den eingehenden und ausgehenden Netzwerkverkehr durch bestimmte Ports des gewählten Datenprotokolls ein.

Alle ausgehenden Verbindungen werden standardmäßig erlaubt (Standardeinstellung der Aktionen), sofern keine entsprechende Verbotsregeln für die Firewall-Verwaltung angegeben sind. Die Standardaktion wird mit niedrigster Priorität ausgeführt: wenn keine andere Netzwerkpaketregel ausgelöst wurde, oder wenn keine Netzwerkpaketregeln angegeben sind, wird die Verbindung erlaubt.

In der Firewall-Verwaltung sind bestimmte Netzwerkpaketregeln standardmäßig angegeben. Sie können Ihre eigenen Netzwerkpaketregeln erstellen und für jede Netzwerkpaketregel eine Ausführungspriorität festlegen.

Über dynamische Regeln

Mit Kaspersky Endpoint Security können Sie der Firewall *dynamische Regeln*, die für eine ordnungsgemäße Ausführung der Anwendung erforderlich sind, hinzufügen oder diese löschen. Beispielsweise fügt der Administrationsagent dynamische Regeln hinzu, die Verbindungen mit Kaspersky Security Center erlauben, die sowohl von der Anwendung als auch von Kaspersky Security Center initiiert werden. Die Regeln zum Schutz vor Verschlüsselung sind ebenfalls dynamisch.

Wenn Kaspersky Endpoint Security im Light Agent-Modus verwendet wird, werden der Firewall automatisch dynamische Regeln hinzugefügt, die Verbindungen zur SVM und zum Integrationsserver ermöglichen.

Kaspersky Endpoint Security überwacht keine dynamischen Regeln und blockiert keinen Zugriff auf Netzwerkressourcen für die Komponenten der Anwendung. Dynamische Regeln hängen nicht vom Status der Komponente "Firewall-Verwaltung" (gestartet/beendet) oder den Änderungen ihrer Ausführungseinstellungen ab. Die Ausführungspriorität für dynamische Regeln ist höher als die Priorität für Netzwerkpaketregeln. Die Anwendung stellt die Auswahl von dynamischen Regeln wieder her, wenn eine davon beispielsweise mithilfe des Tools iptables gelöscht wurde.

Sie können den Satz dynamischer Regeln anzeigen (mithilfe des Befehls `kesl-control -F --query`); die Einstellungen der dynamischen Regeln können jedoch nicht geändert werden.

Über vorinstallierte verfügbare Netzwerke

Ein *verfügbares Netzwerk* ist eine angegebene Gruppe von IP-Adressen oder Subnetzen. Mit einem verfügbaren Netzwerk können Sie dieselben Regeln für mehrere IP-Adressen oder Subnetze verwenden, anstatt separate Regeln für jede IP-Adresse oder jedes Subnetz zu erstellen. Das verfügbare Netzwerk kann beim Erstellen einer Netzwerkpaketregel als Wert für den Parameter "Remote-Adresse" verwendet werden. Kaspersky Endpoint Security verwendet drei vorinstallierte Netzwerke:

- **Öffentlich**. Ein Netzwerk, das nicht durch eine Antiviren-Anwendung, Firewall oder Filter geschützt ist (etwa in einem Internet-Café).
- **Lokal**. Netzwerk des Benutzers, das auf diesem Gerät auf Dateien und Drucker zugreifen kann (etwa ein lokales Netzwerk oder Heimnetzwerk).
- **Vertrauenswürdig**. Ein sicheres Netzwerk, in dem die Geräte keinen Angriffen oder unbefugten Datenzugriffsversuchen ausgesetzt sind.

Das Erstellen eines neuen Netzwerks oder das Löschen eines vorinstallierten Netzwerks ist nicht möglich. Sie können einem Netzwerk jedoch IP-Adressen und Subnetze hinzufügen oder diese aus einem Netzwerk löschen.

Firewall-Verwaltung in der Web Console

In der Web Console können Sie die Firewall-Einstellungen in den Richtlinieneigenschaften verwalten (**Programmeinstellungen** → **Kommunikations- und Web-Schutz** → **Firewall**).

Firewall-Verwaltung in der Verwaltungskonsole

In der Verwaltungskonsole können Sie die Einstellungen der Firewall-Verwaltung in den Richtlinieneigenschaften verwalten (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**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.

Parameter	Description
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**

Parameter	Description
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 ICMP-Typ angeben. 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.
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**

Firewall-Verwaltung über die Befehlszeile

Über die Befehlszeile können Sie die Firewall-Verwaltung mithilfe der vordefinierten Aufgabe "Firewall-Verwaltung" (*Firewall_Management*) konfigurieren.

Standardmäßig wird die Aufgabe "Firewall-Verwaltung" nicht gestartet. Sie können diese Aufgabe manuell starten und beenden.

Sie können die Einstellungen 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 erstellten Firewall-Regeln mit dem Befehl `kesl-control -F --query` an.

Einstellungen der Firewall-Verwaltung

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.

`Protokoll`	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

Parameter	Description	Werte
`ICMPCode`	ICMP-Paketcode. Diese Einstellung kann nur angegeben werden, wenn der Wert der Einstellung `Protocol` auf `ICMP` oder `ICMPv6` festgelegt wurde.	`Any` (Standardwert) – Alle Codes von ICMP-Paketen überwachen. Ganzzahl entsprechend der Spezifikation eines Datentransferprotokolls
`Direction`	Richtung der überwachten Netzwerkaktivität.	`IncomingOutgoing` oder `InOut` (Standardwert) – sowohl eingehende als auch ausgehende Verbindungen überwachen. `Incoming` oder `In` – 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` — Bereich von IPv4-Adressen. `d.d.d.d/p` – Subnetz von Adressen der IPv4-Version, 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` — Bereich von IPv4-Adressen. `d.d.d.d/p` – Subnetz von Adressen der IPv4-Version, 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.

Parameter	Description	Werte
Der Abschnitt **[NetworkZonesPublic]** enthält die Netzwerkadressen, die mit öffentlichen Netzwerken assoziiert sind. Sie können mehrere IP-Adressen oder Subnetze von IP-Adressen angeben.		
`Address.item_#`	Gibt die IP-Adresse oder das IP-Subnetz an.	`d.d.d.d` – Adresse der IPv4-Version, wobei d eine Dezimalzahl von 0 bis 255 ist. `d.d.d.d/p` – Subnetz von Adressen der IPv4-Version, 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 Adressen der IPv4-Version, 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 Adressen der IPv4-Version, 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).

Liste von Regeln für Netzwerkpakete über die Befehlszeile konfigurieren

Um eine Netzwerkpaketregel hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --add-rule [--name <Regelname>] [--action <Aktion>] [--protocol
<Protokoll>] [--direction <Richtung>] [--remote <Remote-Adresse>[:<Port oder
Portbereich>]] [--local <lokale Adresse>[:<Port oder Portbereich>]] [--at <Index>]
```

wobei:

- `--name <Regelname>` ist der Name der Netzwerkpaketregel.
- `--action <Aktion>` – Aktion, die mit den in dieser Netzwerkpaketregel angegebenen Verbindungen ausgeführt wird.

- `--protocol <Protokoll>` ist der Typ des Kommunikationsprotokolls, für das Sie die Netzwerkaktivität überwachen möchten.
- `--direction <Richtung>` – Richtung der überwachten Netzwerkaktivität.
- `--remote <Remote-Adresse [:<Port oder Portbereich>]>` – Netzwerkadresse des Remote-Geräts. Als Remote-Adresse können Sie den Namen einer vordefinierten Netzwerkzone angeben.
- `--local <lokale Adresse [:<Port oder Portbereich>]>` – Netzwerkadresse des Geräts, auf dem Kaspersky Endpoint Security installiert ist.
- `--at <Index>` – Index der Regel in der Liste der Netzwerkpaketregeln. Wenn der Schalter `--at` nicht angegeben wird oder sein Wert größer als die Anzahl der Regeln in der Liste ist, wird die neue Regel zum Ende der Liste hinzugefügt.

Einstellungen, für die Sie im Befehl keine Werte angeben, werden auf ihre Standardwerte gesetzt.

Beispiele:
Führen Sie den folgenden Befehl aus, um eine Regel zu erstellen, die alle eingehenden und hergestellten Verbindungen zum TCP-Port 23 blockiert:

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote
any
```

Führen Sie den folgenden Befehl aus, um eine Regel zu erstellen, die eingehende und hergestellte Verbindungen zum TCP-Port 23 für die Öffentliche Netzwerkzone blockiert:

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote
Public
```

Um eine Netzwerkpaketregel zu löschen, führen Sie einen der folgenden Befehle aus:

- `kesl-control --del-rule --name <Regelname>`
- `kesl-control --del-rule --index <Index>`

wobei:

- `--name <Regelname>` ist der Name der Netzwerkpaketregel.
- `--index <Index>` – Aktueller Index der Regel in der Liste der Netzwerkpaketregeln.

Wenn die Netzwerkpaketregelliste mehrere Regeln mit demselben Namen oder keine Regel mit dem angegebenen Namen oder Index enthält, tritt ein Fehler auf.

Um eine Ausführungspriorität für eine Netzwerkpaketregel zu ändern, führen Sie einen der folgenden Befehle aus:

- `kesl-control --move-rule --name <Regelname> --at <Index>`
- `kesl-control --move-rule --index <Index> --at <Index>`

wobei:

- `--name <Regelname>` ist der Name der Netzwerkpaketregel.
- `--index <Index>` – Aktueller Index der Regel in der Liste der Netzwerkpaketregeln.
- `--at <Index>` – Neuer Regelindex in der Liste der Netzwerkpaketregeln.

Netzwerkzonen über die Befehlszeile konfigurieren

Um eine Netzwerkadresse zur Zone hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --add-zone <Zone> --address <Adresse>
```

wobei:

- `<Zone>` – Vordefinierter Name der Netzwerkzone. Mögliche Werte: `Public`, `Local`, `Trusted`.
- `<Adresse>` – Netzwerkadresse oder Subnetz.

Um eine Netzwerkadresse aus der Zone zu löschen, führen Sie einen der folgenden Befehle aus:

- `kesl-control --del-zone <Zone> --address <Adresse>`
- `kesl-control --del-zone <Zone> --index <Adressindex in der Zone>`

Wenn eine Zone mehrere Elemente mit derselben Netzwerkadresse enthält, wird der Befehl `--del-zone` nicht ausgeführt.

Wenn die angegebene Netzwerkadresse oder der Index nicht existiert, wird eine Fehlermeldung angezeigt.

Schutz vor Web-Bedrohungen

Mit der Komponente „Schutz vor Web-Bedrohungen“ können Sie eingehenden Datenverkehr, der über HTTP-, HTTPS- und FTP-Protokolle übertragen wird, Websites und IP-Adressen untersuchen, das Herunterladen schädlicher Dateien aus dem Internet verhindern und den Zugriff auf Phishing-, Adware- und andere gefährliche Websites blockieren. Der Schutz vor Web-Bedrohungen verwendet Port 9879 für das Abfangen von Verbindungen. Wenn Port 9879 bereits belegt ist, wählt das Programm automatisch einen verfügbaren Port aus, um Verbindungen abzufangen.

Das Unterbrechen oder Starten der Anwendung oder der Schutzkomponente "Schutz vor Web-Bedrohungen" führt dazu, dass Verbindungen auf abgefangenen Ports, wie z. B. HTTPS, unterbrochen werden.

Standardmäßig ist der Schutz vor Web-Bedrohungen deaktiviert. Er wird jedoch automatisch aktiviert, wenn die lokale Verwaltung der Einstellungen für den Schutz vor Web-Bedrohungen auf dem Gerät erlaubt ist (die Richtlinie wird nicht angewendet oder das "Schloss" ist in den Eigenschaften der Richtlinie nicht gesetzt) und wenn eine der folgenden ausführbaren Browserdateien, einschließlich im Snap-Format, im System erkannt wird:

- chrome
- chromium
- chromium-browser
- firefox
- firefox-esr
- google-chrome
- opera
- yandex-browser

Sie können den Schutz vor Web-Bedrohungen ein- und ausschalten und auch Schutzeinstellungen konfigurieren:

- Wählen Sie eine Aktion aus, die von der Anwendung auf eine Webressource angewendet werden soll, auf der ein gefährliches Objekt erkannt wird.
- Konfigurieren Sie eine Liste mit vertrauenswürdigen Webadressen. Die Anwendung untersucht nicht den Inhalt von Websites, deren Webadressen in dieser Liste aufgeführt sind.
- Wählen Sie Objekte aus, welche die Anwendung während der Untersuchung des eingehenden Datenverkehrs erkennen soll.
- Konfigurieren Sie die Untersuchung verschlüsselter Verbindungen, um den HTTPS-Verkehr zu untersuchen.

  Um den FTP-Verkehr zu untersuchen, muss in den Einstellungen zur Untersuchung des Netzwerkverkehrs die Kontrolle aller Netzwerkports konfiguriert werden.

Beim Öffnen einer Website führt die Anwendung folgende Aktionen aus:

1. Sie überprüft die Sicherheit der Website mithilfe der heruntergeladenen Anwendungsdatenbanken.
2. Sie überprüft die Sicherheit der Website mithilfe der **heuristischen Analyse**, sofern diese aktiviert ist.

   Während der heuristischen Analyse analysiert Kaspersky Endpoint Security die Aktivität von Anwendungen im Betriebssystem. Die heuristische Analyse kann gefährliche Objekte erkennen, für die derzeit keine Einträge in den Datenbanken von Kaspersky Endpoint Security vorliegen.
3. Wenn die Verwendung von Kaspersky Security Network aktiviert ist, wird die Zuverlässigkeit einer Website anhand der Reputationsdatenbanken von Kaspersky geprüft.

   Es wird empfohlen, die Verwendung von Kaspersky Security Network zu aktivieren, um die Wirksamkeit des Schutzes vor Web-Bedrohungen zu steigern.
4. Sie blockiert bzw. erlaubt das Öffnen der Website.

Beim Versuch, eine gefährliche Website zu öffnen, führt die Anwendung folgende Aktionen aus:

- Für HTTP- oder FTP-Verkehr blockiert die Anwendung den Zugriff und zeigt eine Warnung an.
- Für HTTPS-Verkehr zeigt der Browser eine Fehlerseite an.

Das Entfernen von Anwendungszertifikaten kann zu einer fehlerhaften Ausführung der Komponente „Schutz vor Web-Bedrohungen“ führen.

Wenn Sie Ausnahmen vom Abfangend es Datenverkehrs mittels Kaspersky Endpoint Security konfiguriert haben, wirken sich diese auf die Funktion der Komponente "Schutz vor Web-Bedrohungen" aus.

Schutz vor Web-Bedrohungen in der Web Console konfigurieren

In der Web Console können Sie in den Eigenschaften der Richtlinie die Einstellungen für den Schutz vor Web-Bedrohungen verwalten (**Programmeinstellungen → Kommunikations- und Web-Schutz → Schutz vor Web-Bedrohungen**).

Schutz vor Web-Bedrohungen in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen für den Schutz vor Web-Bedrohungen in den Eigenschaften der Richtlinie verwalten (Verwalten von Richtlinien in der Verwaltungskonsole, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Basisschutz → Schutz vor Web-Bedrohungen**).

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 Anwendung untersucht nicht den Inhalt von Websites, deren Webadressen in dieser Liste aufgeführt sind.
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 erlaubt den Download 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 der 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.

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 Web-Bedrohungen über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie den Schutz vor Web-Bedrohungen mithilfe der vordefinierten Aufgabe "Schutz vor Web-Bedrohungen" (*Web_Threat_Protection*) verwalten.

Die Aufgabe wird automatisch gestartet, wenn einer der unterstützten Browser im Betriebssystem installiert ist und die lokale Verwaltung der Einstellungen für den Schutz vor Web-Bedrohungen auf dem Gerät zugelassen ist (die Richtlinie wird nicht angewendet oder das "Schloss" ist in den Richtlinieneigenschaften nicht gesetzt). Sie können diese Aufgabe manuell starten und anhalten.

Sie können die Einstellungen für den Schutz vor Web-Bedrohungen konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zum Schutz vor Web-Bedrohungen ändern.

Einstellungen der Aufgabe zum Schutz vor Web-Bedrohungen

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`	Aktiviert oder deaktiviert die Untersuchung von Links gegen Datenbanken mit bösartigen Webadressen.	`Yes` (Standardwert) – Prüfen, ob Links in der Datenbank für bösartige Links aufgeführt sind. `No` – Nicht prüfen, ob Links in der Datenbank für bösartige Links aufgeführt sind.
`CheckPhishing`	Aktiviert oder deaktiviert die Untersuchung von Links gegen Datenbanken mit Phishing-Webadressen.	`Yes` (Standardwert) – Prüfen, ob Links in der Datenbank für Phishing-Links aufgeführt sind. `No` –Nicht prüfen, ob Links in der Datenbank für Phishing-Links aufgeführt sind.
`UseHeuristicForPhishing`	Aktiviert oder deaktiviert die Verwendung der heuristischen Analyse, um Webseiten auf Phishing-Links zu untersuchen.	`Yes` (Standardwert) – Heuristische Analyse zum Erkennen von Phishing-Links verwenden. Bei Angabe dieses Wertes wird als Ebene der heuristischen Analyse `Light` verwendet (die oberflächlichste Untersuchung mit minimaler Systemauslastung). Die Ebene der heuristischen Analyse kann für die Aufgabe zum Schutz vor Web-Bedrohungen nicht geändert werden. `No` – Heuristische Analyse zum Erkennen von Phishing-Links nicht verwenden.
`CheckAdware`	Aktiviert oder deaktiviert die Untersuchung von Links gegen Datenbanken von Adware-Webadressen.	`Yes` – Prüfen, ob Links in der Datenbank für Adware-Links aufgeführt sind. `No` (Standardwert) – Prüfen, ob Links in der Datenbank für Webadressen mit Werbeinhalten aufgeführt sind.

Parameter	Description	Werte
`CheckOther`	Aktiviert oder deaktiviert die Untersuchung von Links gegen Datenbanken von Webadressen, die legitime Anwendungen enthalten, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können.	`Yes` – Untersucht, ob Links in den Datenbanken von Webadressen aufgeführt sind, die legitime Anwendungen enthalten, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können. `No` (Standardwert) – Untersucht nicht, ob Links in den Datenbanken von Webadressen aufgeführt sind, die legitime Anwendungen enthalten, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können.
`UseTrustedAddresses`	Aktiviert und deaktiviert die Verwendung einer Liste vertrauenswürdiger Webadressen. Die Anwendung untersucht vertrauenswürdige Webadressen nicht auf Viren und andere schädliche Objekte. Sie können vertrauenswürdige Webadressen mit dem Parameter `TrustedAddresses.item_#` angeben.	`Yes` (Standardwert) – Eine Liste mit vertrauenswürdigen Webadressen verwenden. `No` – Keine Liste mit vertrauenswürdigen Webadressen verwenden.
`TrustedAddresses.item_#`	Legt die vertrauenswürdigen Webadressen fest.	Der Standardwert ist nicht angegeben. Für die Angabe der Webadressen können Sie **Masken** verwenden. Sie können beim Erstellen einer Adressmaske das Sternchen (*) als Platzhalter für ein oder mehrere Zeichen verwenden. Wenn Sie also die Adressmaske *abc* eingeben, wird sie auf alle Webressourcen angewendet, welche die Sequenz abc enthalten (z. B. www.virus.com/download_virus/page_0-9abcdef.html). Um das Sternchen als Zeichen und nicht als Maske in die Adressmaske aufzunehmen, geben Sie das Zeichen * zweimal ein (z. B. wird mit www.virus.com/**/page_0-9abcdef.html der Link www.virus.com/*/page_0- 9abcdef.html dargestellt). IP-Adressen können nicht mit Masken beschrieben werden.

Netzwerkverkehr untersuchen

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. Die Komponenten "Schutz vor Web-Bedrohungen", "Schutz vor E-Mail-Bedrohungen" und "Web-Kontrolle" können den Netzwerkverkehr entschlüsseln und untersuchen. Standardmäßig ist die Untersuchung verschlüsselter Verbindungen aktiviert.

Sie können die folgenden Parameter der Untersuchung des Netzwerkverkehrs konfigurieren:

- Die Untersuchung verschlüsselter Verbindungen aktivieren oder deaktivieren.
- Wählen Sie die Aktion aus, welche die Anwendung ausführen soll, wenn sie ein nicht vertrauenswürdiges Zertifikat erkennt.
- Wählen Sie die Aktion aus, welche die Anwendung ausführen soll, wenn auf einer Seite ein Fehler bei der Untersuchung des Netzwerk-Datenverkehrs auftritt.
- Aktivieren und deaktivieren Sie die Internetnutzung bei der Untersuchung von Zertifikaten.
- Zeigen Sie eine Liste vertrauenswürdiger Domänen an und konfigurieren Sie sie. Die Anwendung untersucht keine Verbindungen, die beim Aufruf bestimmter Domänen hergestellt wurden.
- Konfigurieren Sie die Stammzertifikate, welche die Anwendung während der Untersuchung verschlüsselter Verbindungen als vertrauenswürdig erachten soll.
- Ausnahmen für die Datenverkehrsüberwachung konfigurieren Sie können Verbindungen angeben, die von der Datenverkehrsüberwachung ausgeschlossen werden sollen. Die ausgeschlossene Verbindung wird durch die folgenden Parameter definiert:
  - Richtung des Datenverkehrs – eingehend oder ausgehend.
  - IP-Adresse des Remote-Geräts – die IP-Adresse, von oder zu welcher der Datenverkehr nicht abgefangen wird (je nach Richtung des Datenverkehrs).
  - 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).

Ausnahmen vom Abfangen des Datenverkehrs gelten nur für TCP-Verbindungen und haben keinen Einfluss auf die Funktionsweise der Netzwerkpaketregeln. Die Ausnahmen vom Abfangen des Datenverkehrs wirken sich auf die Funktion der Schutzkomponenten Schutz vor Web-Bedrohungen, Schutz vor Netzwerkbedrohungen und Web-Kontrolle aus.

Sie können für Kaspersky Endpoint Security auch mit den Tools des Betriebssystems Ausnahmen für das Abfangen des Datenverkehrs konfigurieren.

- Konfigurieren Sie die Liste der von der Anwendung gesteuerten Netzwerkports. Sie können bestimmte Netzwerkports oder Bereiche von Netzwerkports angeben, die untersucht werden sollen.

  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.

- Wählen Sie den von der Anwendung verwendeten Modus zum Abfangen des Datenverkehrs aus.

Beim Ändern der Einstellungen zur Untersuchung des Netzwerkverkehrs generiert die Anwendung das Ereignis *NetworkSettingsChanged*.

Über den Modus zum Abfangen des Datenverkehrs

Die Anwendung kann einen von zwei Modi zum Abfangen des Netzwerkverkehrs verwenden:

- *eBPF-Technologie verwenden*. Wenn dieser Modus ausgewählt ist, verwendet die Anwendung die eBPF-Technologie zum Abfangen des Datenverkehrs. Wenn das Programm die eBPF-Technologie nicht zum Abfangen des Netzwerkverkehrs verwenden kann, wird stattdessen das Dienstprogramm iptables verwendet.

- *iptables-Tool verwenden*. Wenn dieser Modus ausgewählt ist, verwendet die Anwendung das iptables-Tool zum Abfangen des Datenverkehrs. Standardmäßig ist dieser Modus ausgewählt.

Im Modus **eBPF-Technologie verwenden** erstellt das Programm einen eigenen separaten Netzwerk-Namensraum (network linux namespace), in dem 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 Paar "kesl_in – kesl_worm_in" überträgt Netzwerkverkehr für eingehende Verbindungen.

- Das Paar "kesl_out – kesl_worm_out" überträgt Netzwerkverkehr für ausgehende 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.

Wenn Ihr Gerät anfällig für Port-Enumeration-Angriffe ist (z. B. wenn auf dem lokalen Gerät eine Betriebssystem-Firewall mit Portfilterung konfiguriert ist), wird die Auswahl des Modus **eBPF-Technologie verwenden** nicht empfohlen. Auch für Geräte am Netzwerkperimeter der Organisation wird von der Verwendung dieses Modus zum Abfangen des Netzwerkverkehrs abgeraten.

Wenn sich das Gerät in einem isolierten Netzwerksegment, in einem lokalen Netzwerk oder innerhalb des Netzwerkperimeters der Organisation befindet, ist die Auswahl des Modus **eBPF-Technologie verwenden** zum Abfangen des Netzwerkverkehrs zulässig.

Sie können den Modus zum Abfangen des Netzwerkverkehrs in der Web Console, in der Verwaltungskonsole und über der Befehlszeile auswählen.

Um den Modus zum Abfangen des Datenverkehrs zu ändern, muss die Anwendung neu gestartet werden. Während des Neustarts werden bestehende Netzwerkverbindungen unterbrochen.

Untersuchung des Netzwerkverkehrs in der Web Console konfigurieren

In der Web Console können Sie die Einstellungen für die Untersuchung des Netzwerkverkehrs in den Richtlinieneigenschaften verwalten (**Programmeinstellungen** → **Allgemeine Einstellungen** → **Netzwerkeinstellungen** und **Programmeinstellungen** → **Vertrauenswürdige Zone**).

Untersuchung des Netzwerkverkehrs in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen für die Untersuchung des Netzwerkverkehrs in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) verwalten (**Sicherheitskontrolle** → **Netzwerkeinstellungen**).

Einstellungen geschützter Verbindungen

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.

Parameter	Description
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.

Fenster "Überwachte Ports"

Einstellungen der Netzwerkports

Parameter	Description
Alle Netzwerkports überwachen	Wenn diese Aktion ausgewählt ist, überwacht die Anwendung 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.

Untersuchung des Netzwerkverkehrs über die Befehlszeile konfigurieren

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. Diese Datei können Sie verwenden, um Parameter zu 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.
- Einzelne Parameter mittels Schlüssels aus der Befehlszeile wie folgt ändern: `<Name des Parameters>=<Wert des Parameters>`. 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]
```

wobei `--json` angegeben wird, 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 <Pfad zur Konfigurationsdatei> [--json]
```

wobei:

- `--file <Pfad der Konfigurationsdatei>` – Pfad der Datei, in der die Einstellungen der 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` wird angegeben, um die Einstellungen im JSON-Format auszugeben. 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 Befehl aus:

```
kesl-control --set-net-settings --file <Pfad der Konfigurationsdatei> [--json]
```

wobei:

- `--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei mit den Einstellungen zur 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 <Name der Einstellung>=<Wert der Einstellung> [<Name der Einstellung>=<Wert der Einstellung>]
```

`<Name der Einstellung>=<Wert der Einstellung>` – Name und Wert einer der Einstellungen zur Untersuchung des Netzwerkverkehrs.

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 Anwendung hinzugefügten Untersuchungsausschlüsse für verschlüsselte Verbindungen anzuzeigen:

```
kesl-control -N --query user
```

Führen Sie den folgenden Befehl aus, um die Liste der von der Anwendung 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 Anwendungsdatenbanken abgerufen wurden:

```
kesl-control -N --query kl
```

Um die Liste der Domänen zu löschen, welche die Anwendung automatisch von der Untersuchung ausgeschlossen hat, führen Sie den folgenden Befehl aus:

```
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 <Pfad des Zertifikats>
```

wobei:

`<Pfad des Zertifikats>` – Pfad der 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 <Antragsteller des Zertifikats>
```

Um die Liste der vertrauenswürdigen Stammzertifikate anzuzeigen, führen Sie den folgenden Befehl aus:

```
Befehl 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-Adresse> --dst-port <Zielport>
```

wobei:

- `<in|out>` – Richtung des Datenverkehrs der ausgeschlossenen Verbindung. Sie können eine Ausnahme für eingehenden oder ausgehenden Datenverkehr einrichten.
- `< 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.

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:

```
Befehl 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-
Adresse > --dst-port < Zielport >
```

wobei:

- `<in|out>` – Richtung des Datenverkehrs der ausgeschlossenen Verbindung.
- `< Remote-IP-Adresse >` – Adresse des Remote-Geräts im IPv4- oder IPv6-Format, deren Datenverkehr (abhängig von der Richtung des Datenverkehrs) vom Abfangen ausgeschlossen ist.
- `< Zielport >` – Port auf dem geschützten Gerät (bei Ausschluss eingehenden Datenverkehrs) oder Port auf dem Remote-Gerät (bei Ausschluss ausgehenden Datenverkehrs).

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.

> Wenn die Anwendung die eBPF-Technologie zum Abfangen des Datenverkehrs verwendet, werden die kesl_bypass-Regeln nicht angewendet.

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.

Beispielsweise können Sie der kesl_bypass-Kette eine Regel 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.

Schutz vor Netzwerkbedrohungen

Die Komponente "Schutz vor Netzwerkbedrohungen" untersucht den eingehenden Netzwerkdatenverkehr auf Aktivitäten, die für Netzwerkangriffe typisch sind.

Die Anwendung untersucht den eingehenden Datenverkehr für TCP-Ports, deren Nummern Kaspersky Endpoint Security aus den aktuellen Anwendungsdatenbanken erhält. Der Schutz vor Netzwerkbedrohungen verwendet Port 9789 für das Abfangen von Verbindungen.

Zur Untersuchung des Netzwerkverkehrs akzeptiert die Komponente zum Schutz vor Netzwerkbedrohungen Verbindungen von allen Ports, deren Nummern sie aus den Datenbanken der Anwendung erhält. Bei der Untersuchung des Netzwerkes können auf Geräten geöffnete Ports auftauchen, die von keiner Anwendung auf diesem System verwendet werden. Es wird empfohlen, nicht verwendetet Ports mittels Firewall zu schließen.

Aktuelle Verbindungen für abgefangene TCP-Ports werden zurückgesetzt, wenn der Schutz vor Netzwerkbedrohungen aktiviert ist.

Wenn der Schutz vor Netzwerkbedrohungen aktiviert ist und ein versuchter Netzwerkangriff auf ein geschütztes Gerät erkannt wird, blockiert die Anwendung die Netzwerkaktivität des angreifenden Geräts und generiert das Ereignis *Netzwerkangriff erkannt*. Das Ereignis enthält Informationen über das angreifende Gerät. Standardmäßig wird der Netzwerkverkehr des angreifenden Geräts für eine Stunde blockiert. Nach Ablauf der Sperrzeit entsperrt die Anwendung das Gerät.

Der Schutz vor Netzwerkbedrohungen ist standardmäßig deaktiviert.

Sie können den Schutz vor Netzwerkbedrohungen ein- und ausschalten und auch Schutzeinstellungen konfigurieren:

- Wählen Sie die Aktion aus, welche die Anwendung ausführen soll, wenn sie eine für Netzwerkangriffe typische Netzwerkaktivität erkennt.
- Aktivieren und deaktivieren Sie das Blockieren der Netzwerkaktivität, wenn ein versuchter Netzwerkangriff erkannt wird.
- Legen Sie die Dauer der Blockierung des angreifenden Geräts fest.
- Konfigurieren Sie eine Liste von IP-Adressen, deren Netzwerkaktivität nicht durch die Anwendung blockiert wird.

Mithilfe der Befehle zur Verwaltung blockierter Geräte in der Befehlszeile können Sie die Liste der blockierten Geräte anzeigen und diese Geräte manuell entsperren. Kaspersky Security Center verfügt über keine Tools zur Überwachung und Verwaltung blockierter Geräte, mit Ausnahme der Ereignisse *Netzwerkangriff erkannt*.

Wenn Sie Ausnahmen vom Abfangen des Datenverkehrs mittels Kaspersky Endpoint Security konfiguriert haben, wirken sich diese auf die Funktion der Komponente "Schutz vor Web-Bedrohungen" aus.

Schutz vor Netzwerkbedrohungen in der Web Console konfigurieren

In der Web Console können Sie die Einstellungen für den Schutz vor Netzwerkbedrohungen in den Richtlinieneigenschaften verwalten (**Programmeinstellungen** → **Kommunikations- und Web-Schutz** → **Schutz vor Netzwerkbedrohungen**).

Schutz vor Netzwerkbedrohungen in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen für den Schutz vor Netzwerkbedrohungen in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) 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 die Anwendung 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.

Schutz vor Netzwerkbedrohungen über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie den Schutz vor Netzwerkbedrohungen mithilfe der vordefinierten Aufgabe "Schutz vor Netzwerkbedrohungen" (*Network_Threat_Protection*) verwalten.

Die Aufgabe zum Schutz vor Netzwerkbedrohungen wird standardmäßig nicht gestartet. Sie können diese Aufgabe manuell starten und anhalten.

Sie können die Einstellungen für den Schutz vor Netzwerkbedrohungen konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zum Schutz vor Netzwerkbedrohungen ändern.

Einstellungen der Aufgabe zum Schutz vor Netzwerkbedrohungen

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 Adressen der IPv4-Version, 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.

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 Ihr Gerät mithilfe von Antiviren-Datenbanken, dem Cloud-Dienst Kaspersky Security Network und der heuristischen Analyse.

Der Schutz vor E-Mail-Bedrohungen kann sowohl eingehende als auch ausgehende Nachrichten untersuchen.

Die Anwendung unterstützt die Protokolle POP3, SMTP und IMAP für alle E-Mail-Clients und die erweiterten Protokollvarianten POP3S, SMTPS und IMAPS für die E-Mail-Clients MyOffice Mail und Organizer R7-Office. Andere Protokolle werden vom Schutz vor E-Mail-Bedrohungen nicht unterstützt.

Damit der Schutz vor E-Mail-Bedrohungen funktioniert, müssen in den Netzwerkeinstellungen die Netzwerkports 25, 465, 587, 110, 995, 143 und 993 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. Sie können den Schutz vor E-Mail-Bedrohungen über die Web Console, die Verwaltungskonsole und die Befehlszeile aktivieren, deaktivieren und konfigurieren.

Schutz vor E-Mail-Bedrohungen in der Web Console konfigurieren

In der Web Console können Sie Einstellungen des Schutzes vor E-Mail-Bedrohungen in den Richtlinieneigenschaften konfigurieren (**Anwendungseinstellungen** → **Kommunikations- und Web-Schutz** → **Schutz vor E-Mail-Bedrohungen**).

Verwaltungskonsole in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen für den Schutz vor E-Mail-Bedrohungen in den Richtlinieneigenschaften verwalten (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Basisschutz** → **Schutz vor E-Mail-Bedrohungen**).

Einstellungen der Komponente zum 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 (Anhangsfilter)	Durch Klicken auf die Schaltfläche öffnet sich das Fenster **Anhangsfilter**, in dem Sie die Filterung von E-Mail-Anhängen konfigurieren können.

Parameter	Description
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. Entfernen, 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.

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 **Eingehende 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.
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 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.
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 E-Mail-Bedrohungen über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie den Schutz vor E-Mail-Bedrohungen mithilfe der vordefinierten Aufgabe "Schutz vor E-Mail-Bedrohungen" (*Mail_Monitoring*) verwalten.

Die Aufgabe "Schutz vor E-Mail-Bedrohungen" wird standardmäßig gestartet. Sie können diese Aufgabe manuell starten und beenden.

Die Rechte der Administrator-Rolle sind erforderlich, um die Aufgabe zum Schutz vor E-Mail-Bedrohungen über die Befehlszeile zu starten und zu beenden.

Sie können die Einstellungen für den Schutz vor E-Mail-Bedrohungen konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zum Schutz vor E-Mail-Bedrohungen ändern.

Die untere Tabelle beschreibt die verfügbaren Werte und Standardwerte der Einstellungen, die Sie für die Aufgabe zum Schutz vor E-Mail-Bedrohungen angeben können.

Einstellungen der Aufgabe zum Schutz vor E-Mail-Bedrohungen

Parameter	Description	Werte
`CheckIncomingMessagesOnly`	Der *Schutzbereich* umfasst die Objekte, die von der Komponente während ihrer Ausführung untersucht werden: eingehende und ausgehende Nachrichten oder nur eingehende Nachrichten.	`Yes` – Die Anwendung untersucht nur eingehende Nachrichten. `No` (Standard) – Die Anwendung untersucht eingehende und ausgehende Nachrichten.
`ScanFileArchive`	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.	`Yes` (Standard) – Die Anwendung untersucht verschachtelte Archive. `No` – Die Anwendung untersucht keine verschachtelten Archive.
`ScanFileOffice`	Aktiviert oder deaktiviert die Untersuchung angehängter Office-Dateien.	`Yes` (Standard) – Die Anwendung untersucht angehängte Office-Dateien. `No` – Die Anwendung untersucht keine angehängten Office-Dateien.
`UseSizeLimit`	Begrenzt die Größe für zu untersuchende, angehängte Archive	`Yes` – Die Anwendung schließt von der Untersuchung der an E-Mail-Nachrichten angehängten Archive jene Archive aus, deren Größe den im Argument `SizeLimit` angegebenen Wert übersteigt. `No` (Standard) – Die Anwendung untersucht Archive beliebiger Größe, die an E-Mail-Nachrichten angehängt sind.
`SizeLimit`	Legt die maximale Größe der zu untersuchenden angehängten Archive fest.	1 – 9999 MB.
`UseTimeLimit`	Begrenzt die maximale Dauer der Untersuchung angehängter Archive.	`Yes` – Die Anwendung beendet die Untersuchung angehängter Archive nach der im Argument `TimeLimit` festgelegten Zeit. `No` (Standard) – Die Zeit für die Untersuchung angehängter Archive ist nicht begrenzt.
`TimeLimit`	Legt die maximale Dauer der Untersuchung angehängter Archive fest.	1 – 9999 Sek.
`ExtensionFilter`	Konfiguriert den Anhangsfilter von E-Mail-Anhängen.	`Disable` – Die Anwendung filtert keine Dateien, die an E-Mail-Nachrichten angehängt sind. `Rename` (Standard) – Die Anwendung ersetzt das letzte Zeichen in der Dateierweiterung angehängter Dateien, die den angegebenen Typen entsprechen, mit einem Unterstrich (Bsp.: attachment.doc_). Wenn ein Benutzer die Datei öffnen möchte, muss er sie daher zunächst umbenennen. `Delete` – Die Anwendung löscht aus E-Mail-Nachrichten jene Dateien, die den angegeben Typen entsprechen.

Parameter	Description	Werte

`ExtensionMasks`	Legt die Dateierweiterungen für Anhänge fest, die umbenannt oder aus E-Mail-Nachrichten entfernt werden sollen.	Eine Liste mit mehreren Erweiterungen wird wie folgt angegeben:
		`[ExtensionMasks.item_0000]`
		`UseExtensionMask=Yes`
		`ExtensionMask=*.txt`
		`[ExtensionMasks.item_0001]`
		`UseExtensionMask=Yes`
		`ExtensionMask=*.run`
		`[ExtensionMasks.item_0002]`
		`UseExtensionMask=Yes`
		`ExtensionMask=*.exe`
		`...`
		Standardmäßig werden Dateien mit den folgenden Erweiterungen verarbeitet: TXT, RUN, EXE, JS, JSE, MSI, SCR, VBE, VBS, SH.
		Um die Liste der Dateierweiterungen zu ändern, müssen Sie die Aufgabenparameter in eine INI-Datei exportieren. Anschließend können Sie die Liste in dieser Datei bearbeiten und die INI-Datei wieder in die Anwendung importieren.

`UseAnalyzer`	Aktiviert oder deaktiviert die Verwendung der heuristischen Analyse.	`Yes` (Standard) – Die heuristische Analyse ist aktiviert. `No` – Die heuristische Analyse ist deaktiviert.
`AnalyzerLevel`	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.	`Leicht` – Am wenigsten genaue Untersuchung, minimale Systembelastung. `Medium` (Standard) – Mittlere Untersuchung, ausgeglichene Systembelastung. `Tief` – Genaueste Untersuchung, maximale Systembelastung.
`ActionOnThreat`	Die Aktion, die der Schutz vor E-Mail-Bedrohungen anwendet, wenn eine Bedrohung in eingehenden E-Mail-Nachrichten erkannt wird. Der Parameter `ActionOnThreat` wird auf ausgehende Nachrichten nicht angewendet. Wenn in einer ausgehenden Nachricht ein infiziertes Objekt entdeckt wird, blockiert die Anwendung den Versand der Nachricht.	`DisinfectDeleteIfNotPossible` (Standard) – Desinfizieren. Entfernen, 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. `DisinfectBlockIfNotPossible` – 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. `Block` – 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.

Schutz vor BadUSB-Angriffen

Bestimmte Viren verändern die in USB-Geräten eingebettete Software so, dass das USB-Gerät vom Betriebssystem als Tastatur erkannt wird. Dadurch kann der Virus Befehle unter Ihrem Benutzerkonto ausführen, z. B. eine schädliche Anwendung herunterladen.

Die Komponente Schutz vor BadUSB-Angriffen verhindert, dass sich infizierte USB-Geräte mit Ihrem Gerät verbinden und sich als Tastatur ausgeben.

Wenn ein vom Betriebssystem als Tastatur erkanntes USB-Gerät angeschlossen wird, fordert die Anwendung den Benutzer auf, einen von der Anwendung generierten numerischen Code über die Tastatur oder die Bildschirmtastatur (falls verfügbar) einzugeben. Dieser Vorgang heißt Autorisierung der Tastatur.

Wenn der Code korrekt eingegeben wird, speichert die Anwendung die Parameter zum Identifizieren der Tastatur (deren VID/PID und die angeschlossene Portnummer) in der Liste der autorisierten Tastaturen. Wenn die Tastatur erneut angeschlossen oder das Betriebssystem neu gestartet wird, muss die Tastatur nicht mehr autorisiert werden.

> Wird eine autorisierte Tastatur an einen anderen USB-Port des Geräts angeschlossen, fordert die Anwendung erneut eine Autorisierung an.

Wenn der Code falsch eingegeben wird, generiert die Anwendung einen neuen. Sie können die Anzahl der Eingabeversuche des Codes konfigurieren. Wird der Code mehrmals falsch eingegeben oder das Fenster zur Autorisierung der Tastatur geschlossen, sperrt die Anwendung die Eingabe über diese Tastatur. Nach Ablauf der Blockierungszeit für USB-Geräte oder wenn das Betriebssystem neu gestartet wird, schlägt das Programm erneut vor, die Autorisierung vorzunehmen.

Das Programm erlaubt die Verwendung einer autorisierten Tastatur. Eine Tastatur, die nicht autorisiert wurde, wird blockiert.

Die Komponente "Schutz vor BadUSB-Angriffen" ist standardmäßig deaktiviert. Sie können den Schutz vor BadUSB-Angriffen über die Web Console, die Verwaltungskonsole und die Befehlszeile aktivieren, deaktivieren und konfigurieren.

Schutz vor BadUSB-Angriffen in der Web Console konfigurieren

In der Web Console können Sie die Parameter des Schutzes vor BadUSB-Angriffen in den Richtlinieneigenschaften konfigurieren (**Anwendungseinstellungen** → **Host-Schutz** → **Schutz vor BadUSB-Angriffen**).

Schutz vor BadUSB-Angriffen in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen für Schutz vor Web-Bedrohungen in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Basisschutz** → **Schutz vor BadUSB-Angriffen**) verwalten.

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 an Versuchen zur Autorisierung für ein USB-Gerät:	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.
Blockieren des Geräts beim Erreichen der maximalen Anzahl an Autorisierungsversuchen (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). Standardwert: 5.
Verwendung der Bildschirmtastatur zur Autorisierung von USB-Geräten verbieten	Ist das Kontrollkästchen aktiviert, so verbietet das Programm die Verwendung einer Bildschirmtastatur für die Autorisierung eines USB-Geräts, von dem aus der Autorisierungscode nicht eingegeben werden kann. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Schutz vor BadUSB-Angriffen über die Befehlszeile konfigurieren

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.

Schutz vor bösartiger Remote-Verschlüsselung

Die Komponente "Schutz vor Verschlüsselung" ermöglicht Ihnen, Ihre Dateien in den lokalen Verzeichnissen mit Netzwerkzugang durch SMB-/NFS-Protokolle vor bösartiger Remote-Verschlüsselung zu schützen.

Um die Komponente nutzen zu können, benötigen Sie eine Lizenz, in der diese Funktionalität enthalten ist.

Wenn der Schutz vor Verschlüsselung aktiviert ist, prüft Kaspersky Endpoint Security die Aktionen von Remote-Geräten mit Dateiressourcen, die sich in freigegebenen Netzwerkverzeichnissen des geschützten Geräts befinden, auf bösartige Verschlüsselung. Wenn die Anwendung die Aktionen eines Remote-Geräts, das auf freigegebene Netzwerkressourcen zugreift, als bösartige Verschlüsselung interpretiert, erstellt und aktiviert die Anwendung eine Regel für die Firewall des Betriebssystems, die den Netzwerkverkehr vom gefährdeten Gerät blockiert. Das kompromittierte Gerät wird zur Liste der nicht vertrauenswürdigen Geräte hinzugefügt und der Zugriff auf freigegebene Netzwerkverzeichnisse für alle nicht vertrauenswürdigen Geräte wird blockiert. Die App generiert das Ereignis *Verschlüsselung erkannt*, das Informationen über das gefährdete Gerät enthält.

Standardmäßig blockiert die Anwendung den Zugriff von nicht vertrauenswürdigen Computern auf freigegebene Netzwerkordner für 30 Minuten. Nach Ablauf der Sperrzeit entfernt die Anwendung das gefährdete Gerät aus der Liste der nicht vertrauenswürdigen Geräte und der Zugriff des Geräts auf freigegebene Netzwerkordner wird automatisch wiederhergestellt.

Firewall-Regeln, die von der Komponente "Schutz vor Verschlüsselung" erstellt wurden, können nicht mithilfe des Tools "iptables" gelöscht werden, da die Anwendung die Regeln jede Minute wiederherstellt.

Standardmäßig ist der Schutz vor bösartiger Remote-Verschlüsselung deaktiviert.

Sie können den Schutz vor bösartiger Verschlüsselung ein- und ausschalten und auch Schutzeinstellungen konfigurieren:

- Wählen Sie die Aktion aus, die von der Anwendung ausgeführt werden soll, wenn eine Verschlüsselung erkannt wird: Den Benutzer informieren oder das Gerät blockieren, das eine böswillige Verschlüsselung durchführt.

  Wenn die Aktion *Informieren* ausgewählt wurde, untersucht die Anwendung die Aktionen von Remote-Geräten mit freigegebenen Netzwerkordnern trotzdem auf bösartige Verschlüsselung, wenn die Aufgabe zum Schutz vor Verschlüsselung ausgeführt wird. Sollte eine bösartige Verschlüsselung erkannt werden, wird das Ereignis *Verschlüsselung erkannt* erstellt, das kompromittierte Gerät wird jedoch nicht blockiert.

- Legen Sie die Dauer für die Blockierung eines nicht vertrauenswürdigen Geräts fest.

- Geben Sie Dateien und Verzeichnisse an, welche die Anwendung vor bösartiger Verschlüsselung schützt.

- Geben Sie Dateien und Verzeichnisse an, die vom Schutz vor bösartiger Verschlüsselung ausgeschlossen sind.

  Die Anwendung stuft eine Aktivität nicht als Verschlüsselung ein, wenn die Verschlüsselungsaktivität in Verzeichnissen entdeckt wird, die vom Schutz vor Verschlüsselung ausgeschlossen sind.

Mithilfe der Befehle zur Verwaltung blockierter Geräte in der Befehlszeile können Sie die Liste der blockierten Geräte anzeigen und diese Geräte manuell entsperren. Kaspersky Security Center verfügt über keine Tools zur Überwachung und Verwaltung blockierter Geräte, mit Ausnahme der Ereignisse *Verschlüsselung erkannt*.

Damit die Komponente "Schutz vor Verschlüsselung" ordnungsgemäß ausgeführt werden kann, muss mindestens einer der folgenden Dienste im Betriebssystem installiert sein: Samba oder NFS. Für den NFS-Dienst muss das Paket rpcbind installiert sein.

Die Komponente "Schutz vor Verschlüsselung" wird mit den Protokollen SMB1, SMB2, SMB3, NFS3, TCP/UDP und IP/IPv6 korrekt ausgeführt. Die Protokolle NFS2 und NFS4 werden nicht unterstützt. Es wird empfohlen, dass Sie Ihre Server-Einstellungen so konfigurieren, dass NFS2- und NFS4-Protokolle nicht zum Mounten von Ressourcen verwendet werden können.

Die Anwendung "Kaspersky Endpoint Security" blockiert den Zugriff auf die freigegebenen Netzwerkordner erst dann, wenn die Aktivitäten des Geräts als bösartig eingestuft wurden. Es wird daher mindestens eine Datei verschlüsselt, bevor die Anwendung eine bösartige Aktivität erkennt.

Schutz vor Verschlüsselung in der Web Console konfigurieren

In der Web Console können Sie in den Richtlinieneigenschaften (**Programmeinstellungen** → **Host-Schutz** → **Verhaltensanalyse** → **Schutz vor Verschlüsselung**) die Einstellungen für den Schutz vor Verschlüsselung verwalten.

Schutz vor Verschlüsselung in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Richtlinie mithilfe der Verwaltungskonsole erstellen) (**Erweiterter Schutz** → **Schutz vor Verschlüsselung**) die Einstellungen für den Schutz vor Verschlüsselung verwalten.

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.

Einstellungen des Untersuchungsbereichs

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 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 den Schutzbereich der Komponente "Schutz vor Verschlüsselung" hinzufügen und bearbeiten.

Einstellungen des Schutzbereichs

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 Anwendung diesen Schutzbereich während der Ausführung der Komponente. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die Anwendung 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.

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** – Lokale Verzeichnisse. • **Freigegeben** – Ressourcen von Server-Dateisystemen, die über das Samba- oder NFS-Protokoll zugänglich sind. • **Alle freigegebenen** (Standardwert) – Alle Ressourcen des Server-Dateisystems, die über das Samba- oder NFS-Protokoll zugänglich sind.
	Wenn in der Drop-down-Liste der Dateisysteme der Typ **Alle** ausgewählt ist, können Sie rechts in der Drop-down-Liste das Protokoll für den Remote-Zugriff auswählen: • **NFS** – Remote-Verzeichnisse, die auf dem Gerät über das NFS-Protokoll eingebunden sind. • **Samba** – Remote-Verzeichnisse, die auf dem Gerät über das Samba-Protokoll eingebunden sind.
	Wenn in der Dropdown-Liste der Dateisysteme der Typ **Lokal** ausgewählt ist, können Sie im Eingabefeld den Pfad zu dem Verzeichnis angeben, das Sie in den Schutzbereich aufnehmen möchten. Bei der Angabe des Pfades können Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld darf nicht leer sein.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der 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.

Fenster "Schutzeinstellungen"

Schutz-Einstellungen

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 Anwendung untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden.

Einstellungen des Ausschlussbereichs

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 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. Sie können spezielle Tags verwenden, um einen Container oder ein Image anzugeben: • `[container-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` Wobei gilt: `<ID>` ist die Container-ID. `<Name>` ist ein Containername `<Pfad zum lokalen Verzeichnis>` 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>]/Pfad zum lokalen Verzeichnis>`. Jede eindeutige Kombination aus 1 bis 4 Tags im Rahmen eines Bereichs ist möglich. Die Reihenfolge der Tags wird dabei ignoriert. Beispiel: • `[container-name:<Name>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` • `[container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[image-name:<Name>][image-id:<ID>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][container-id:<ID>][image-name:<Name>]/<Pfad zum lokalen Verzeichnis>` • `[container-name:<Name>][image-id:<ID>][container-id:<ID>][image-name:<Name>]/Pfad zum lokalen Verzeichnis>` Für den Namen und den Identifikator können Sie Masken (mittels der Symbole `?` und `*`) verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. 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.

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).

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.

Schutz vor Verschlüsselung über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie den Schutz vor Verschlüsselung mithilfe der Aufgabe "Schutz vor Verschlüsselung" (*Anti_Cryptor*) verwalten.

Die Aufgabe zum Schutz vor Verschlüsselung wird standardmäßig nicht gestartet. Sie können diese Aufgabe manuell starten und beenden.

Sie können die Einstellungen für den Schutz vor Verschlüsselung konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zum Schutz vor Verschlüsselung ändern.

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 aus dem Schutzbereich, die in der Einstellung `ExcludeMasks.item_#` angegeben sind. Diese Einstellung funktioniert nur, wenn die Einstellung `ExcludeMasks.item_#` angegeben ist.	`Yes` – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, aus dem Schutzbereich ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht aus dem Schutzbereich ausschließen.
`ExcludeMasks.item_#`	Ausschluss von Objekten aus dem Schutzbereich nach Name oder Maske. Mit dieser Einstellung können Sie eine einzelne Datei anhand des Namens oder mehrere Dateien anhand von Masken im Shell-Format aus dem angegebenen Schutzbereich ausschließen. Bevor Sie den Wert dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseExcludeMasks` aktiviert ist. Wenn Sie mehrere Masken angeben möchten, geben Sie jede Maske in einer neuen Zeile mit einem neuen Index an.	Der Standardwert ist nicht angegeben.
Der Abschnitt **[ScanScope.item_ #]** enthält die Bereiche, die von der 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.	Standardwert: `All shared directories`.
`UseScanArea`	Aktiviert den Schutz des angegebenen Bereichs. Um die Aufgabe auszuführen, müssen Sie mindestens einen zu schützenden Bereich angeben.	`Yes` (Standardwert) – Den angegebenen Bereich schützen. `No` – Den angegebenen Bereich nicht schützen
`AreaMask.item_#`	Einschränkungen des Schutzbereichs. Im Schutzbereich schützt die 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)

Parameter	Description	Werte
`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 Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. `AllShared` (Standardwert) – Alle über SMB/NFS freigegebenen Ressourcen schützen. `Shared:SMB` – 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.	Standardwert: `All objects`
`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).

Parameter	Description	Werte
`Path`	Pfad zum Verzeichnis mit Objekten, die vom Schutz ausgeschlossen sind.	`< Pfad zum lokalen Verzeichnis >` – Objekte im angegebenen Verzeichnis vom Schutz ausschließen. Bei der Angabe des Pfades können Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. `Mounted:NFS` – Remote-Verzeichnisse, die auf dem Client-Gerät über das NFS-Protokoll gemountet sind, vom Schutz ausschließen. `Mounted:SMB` – Remote-Verzeichnisse, die auf Client-Gerät über das Samba-Protokoll gemountet sind, vom Schutz ausschließen. `AllRemoteMounted` – Alle Remote-Verzeichnisse, die auf dem Client-Gerät über Samba- oder NFS-Protokolle gemountet sind, vom Schutz ausschließen.

Blockierte Geräte verwalten

Im Rahmen des Schutzes des Geräts vor Netzwerkbedrohungen und bösartiger Remote-Verschlüsselung kann Kaspersky Endpoint Security Remote-Geräte blockieren, deren Aktionen als bösartig eingestuft werden:

- Wenn eine bösartige Verschlüsselung erkannt wird, blockiert die Anwendung den Zugriff des Remote-Geräts auf freigegebene Netzwerkverzeichnisse des geschützten Geräts.
- Wenn ein versuchter Netzwerkangriff auf ein geschütztes Gerät erkannt wird, blockiert die Anwendung den Netzwerkverkehr vom angreifenden Gerät.

Sie können die Dauer der Blockierung in den Einstellungen zum Schutz vor Netzwerkbedrohungen und Schutz vor bösartiger Remote-Verschlüsselung ändern. Nach Ablauf des angegebenen Zeitraums entsperrt die Anwendung das Gerät.

Wenn Sie die Anwendung über die Befehlszeile verwalten, können Sie mit den Befehlen zur Verwaltung gesperrter Geräte die Liste der Geräte anzeigen, die aufgrund der Ausführung der Anwendung auf dem Gerät gesperrt sind, und diese Geräte manuell entsperren, bevor die Sperrzeit abläuft. Kaspersky Security Center verfügt über keine Tools zur Überwachung und Verwaltung blockierter Geräte, mit Ausnahme der Ereignisse *Netzwerkangriff erkannt* und *Verschlüsselung erkannt*.

Um die Liste mit blockierten Geräten anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-blocked-hosts
```

Als Ergebnis der Ausführung des Befehls gibt die Anwendung die Liste der blockierten Geräte in der Konsole aus.

Um die Blockierung von Geräten aufzuheben, führen Sie den folgenden Befehl aus:

```
kesl-control --allow-hosts <Adresse>
```

Wobei gilt: `<Adresse>` Eine oder mehrere IP-Adressen von Geräten oder Subnetzen (IPv4/IPv6, einschließlich Adresse in Kurzform). Sie können mehrere, durch Leerzeichen getrennte IP-Adressen von Geräten oder Subnetzen angeben.

Als Ergebnis der Ausführung des Befehls entsperrt die Anwendung die angegebenen Geräte.

Beispiele:
IPv4-Adressen:
```
dez – 192.168.0.1
dez – 192.168.0.0/24
```
IPv6-Adressen:
```
hex – FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
hex – FEDC:BA98:7654:3210:FEDC:BA98:7654:3210%1
hex – 2001:db8::ae21:ad12
hex – ::ffff:255.255.255.254
hex – ::
```

Programmkontrolle

Mit der Komponente "Programmkontrolle" können Sie den Start von Anwendungen auf geschützten Geräten überwachen. Die Programmkontrolle reduziert das Risiko einer Geräteinfektion, indem der Benutzerzugriff auf Anwendungen eingeschränkt wird. Mit der Aufgabe Inventarisierung können Sie Informationen zu Anwendungen abrufen, die auf geschützten Geräten installiert sind.

Um die Komponente nutzen zu können, benötigen Sie eine Lizenz, in der diese Funktionalität enthalten ist.

Der Start von Programmen wird durch die *Regeln der Programmkontrolle* geregelt.

Die Komponente "Programmkontrolle" kann in einem von zwei Modi ausgeführt werden:

- *Deny-Liste*. In diesem Modus erlaubt Kaspersky Endpoint Security allen Benutzern das Starten von allen Anwendungen, mit Ausnahme derer, die in den Regeln der Programmkontrolle angegeben sind. Standardmäßig wird die Komponente "Programmkontrolle" in diesem Modus ausgeführt.

- *Allow-Liste*. In diesem Modus verbietet Kaspersky Endpoint Security allen Benutzern das Starten von allen Anwendungen, mit Ausnahme derer, die in den Regeln der Programmkontrolle angegeben sind.

Wenn die Regeln der Programmkontrolle mit maximaler Genauigkeit erstellt wurden, verbietet Kaspersky Endpoint Security zum einen den Start aller neuen, noch nicht vom Administrator des lokalen Unternehmensnetzwerks überprüften Anwendungen, gewährleistet dabei aber zum anderen die Funktionsfähigkeit des Betriebssystems und der bereits untersuchten Anwendungen, die Benutzer für ihre Arbeit benötigen.

Der Administrator von Kaspersky Security Center oder ein lokaler Benutzer mit in der App zugewiesener Rolle admin kann den Start von Prozessen unter dem Root-Konto durch Verwendung der Aufgabe "App-Kontrolle" verbieten oder erlauben.

Standardmäßig ist die Programmkontrolle deaktiviert. Sie können die Programmkontrolle aktivieren und deaktivieren sowie die Ausführungseinstellungen der Komponente konfigurieren:

- Wählen Sie den Modus der Komponente "Programmkontrolle" aus: *Allow-Liste* oder *Deny-Liste*.

- Erstellen Sie Regeln für die Programmkontrolle für jeden Modus der Komponente.

- Wählen Sie die Aktion aus, die Kaspersky Endpoint Security ausführen soll, wenn ein Versuch erkannt wird, eine Anwendung zu starten, die den Regeln entspricht: Kaspersky Endpoint Security kann die *Regeln anwenden* und die in den Regeln festgelegte Aktion ausführen oder die *Regeln testen* und nur über den Versuch, eine Anwendung zu starten, die den Regeln entspricht, informieren.

- Konfigurierte Parameter der Programmkontrolle exportieren und importieren.

Die Programmkontrolle unterstützt keine Startsteuerung für die Anwendungen Snap, Flatpak und AnwendungImage.

Die App-Kontrolle überwacht weder die Ausführung von Skripten aus Interpretern, die nicht von Kaspersky Endpoint Security unterstützt werden, noch die Ausführung von Skripten, die nicht über die Befehlszeile an den Interpreter übergeben werden. Kaspersky Endpoint Security unterstützt die folgenden Interpreter: Python, Perl, Bash, SSH.

Wenn die Regeln für die App-Kontrolle den Start eines Interpreters erlauben, blockiert Kaspersky Endpoint Security keine Skripte, die über diesen Interpreter ausgeführt werden. Wenn die Ausführung von mindestens einem der in der Befehlszeile des Interpreters angegebenen Skripte durch die Regeln für die Programmkontrolle verboten ist, blockiert Kaspersky Endpoint Security alle Skripte, die in der Befehlszeile des Interpreters angegeben sind. Ausnahme: cat script.py | python.

Über die Regeln für die Programmkontrolle

Bei einer *Regel der Programmkontrolle* handelt es sich um eine Reihe von Einstellungen, welche die Bedingungen für das Auslösen der Regel und die Aktionen der Komponente "Programmkontrolle" beim Auslösen der Regel enthalten (Benutzern das Starten der Anwendung erlauben oder verbieten):

- Zugehörigkeit der Anwendung zu den Programmkategorien. Eine *Programmkategorie* ist eine Gruppe von Programmen, die gemeinsame Eigenschaften haben. Darunter fallen z. B. die Kategorie für ausführbare Dateien installierter Anwendungen und die Kategorie für den Standardsatz an notwendigen Anwendungen, die ein Unternehmen in seinem Geschäftsalltag verwendet. Eine Kategorie kann jeweils nur in einer einzigen Regel verwendet werden.

  Die Verwendung der KL-Kategorien von Kaspersky Security Center wird von Kaspersky Endpoint Security nicht unterstützt.

- Das Starten von Anwendungen für ausgewählte Benutzer und/oder Benutzergruppen verbieten oder erlauben. Sie können Benutzer und/oder Benutzergruppen auswählen, denen der Start von Anwendungen aus einer angegebenen Kategorie erlaubt oder verboten werden soll.

- Auslösebedingung für eine Regel. Eine Bedingung ist eine Übereinstimmung nach dem Muster "Bedingungstyp – Bedingungskriterium – Bedingungswert". Basierend auf den Bedingungen der Regelauslösung wendet Kaspersky Endpoint Security die Regel auf eine Anwendung entweder an oder nicht. Regeln verwenden Einschluss- und Ausschlussbedingungen:

  - *Einschlussbedingungen*. Kaspersky Endpoint Security wendet eine Regel auf eine Anwendung an, wenn die Anwendung mindestens eine Einschlussbedingung erfüllt.

  - *Ausschlussbedingungen*. Kaspersky Endpoint Security wendet eine Regel nicht auf eine Anwendung an, wenn die Anwendung mindestens eine Ausschlussbedingung oder keine der Einschlussbedingungen erfüllt.

  Die Bedingungen zum Auslösen der Regel werden anhand der folgenden Kriterien gebildet:

  - Name der ausführbaren Anwendungsdatei.

  - Name des Verzeichnisses mit der ausführbaren Anwendungsdatei.

  - Hash der ausführbaren Anwendungsdatei Es ist nur SHA256 zulässig.

  Für jedes Kriterium, das in einer Bedingung verwendet wird, muss ein Wert angegeben werden.

Um Datei- und Verzeichnisnamen anzugeben, können Sie **Masken** verwenden.

Sie können das Zeichen * (beliebige Zeichenfolge) oder das Zeichen ? (beliebiges einzelnes Zeichen) verwenden, um eine Maske für einen Datei- oder Verzeichnisnamen zu bilden.

Sie können das Zeichen * verwenden, um eine beliebige Anzahl an Zeichen (auch null Zeichen) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/*/file*/` oder `/dir/file*/`.

Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.

Wenn die Einstellungen der ausgeführten Anwendung den in der Einschlussbedingung angegebenen Kriterien entsprechen, wird die Regel ausgelöst. In diesem Fall führt Kaspersky Endpoint Security die in der Regel angegebene Aktion aus. Wenn die Einstellungen den in der Ausschlussbedingung angegebenen Kriterien entsprechen, überwacht Kaspersky Endpoint Security den Start der Anwendung nicht.

Regeln der Programmkontrolle können einen der folgenden *Ausführungsstatus* haben:

- *Aktiviert* – Die Regel ist aktiviert und Kaspersky Endpoint Security wendet diese Regel während der Programmkontrolle an.
- *Deaktiviert*: Die Regel ist deaktiviert und wird nicht auf die Programmkontrolle angewendet.
- *Test* – Kaspersky Endpoint Security erlaubt das Starten von Anwendungen, die den Regelbedingungen entsprechen, registriert aber Informationen über den Start dieser Anwendungen im Bericht.

Der Status der Regel hat eine höhere Priorität als die in der Regel angegebene Aktion.

Testmodus für Regeln der Programmkontrolle

Damit Regeln der Programmkontrolle keine für die Arbeit erforderlichen Programme blockieren, wird empfohlen, den *Test für Regeln der Programmkontrolle* zu aktivieren. In diesem Modus blockiert Kaspersky Endpoint Security die Ausführung von Programmen von Drittanbietern nicht, sendet jedoch 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 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. 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 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 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.

Programmkontrolle in der Web Console konfigurieren

In der Web Console können Sie in den Richtlinieneigenschaften (**Programmeinstellungen** → **Sicherheitskontrolle** → **App-Kontrolle**) die Einstellungen für die Programmkontrolle verwalten.

Programmkontrolle in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen für die Gerätekontrolle in den Eigenschaften der Richtlinie verwalten (Verwalten von Richtlinien in der Verwaltungskonsole, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Sicherheitskontrolle** → **Programmkontrolle**).

Einstellungen der 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 Programmkontrolle 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.

Parameter	Description
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 Programmkontrolle"

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 Programmkontrolle

Parameter	Description
Name der Kategorie	Der Name der Programmkategorie, 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 Programmkontrolle
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.
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 des Assistenten. 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**.

Programmkontrolle über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Programmkontrolle mithilfe der vordefinierten Aufgabe "Programmkontrolle" (*Application_Control*) verwalten.

Standardmäßig wird die Aufgabe "Programmkontrolle" nicht ausgeführt. Sie können diese Aufgabe manuell starten und anhalten.

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 Verwenden von Befehlszeilenoptionen den Befehl `kesl-control --set-settings` mit dem Flag `--accept` aus.

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.

Einstellungen der Aufgabe zur Programmkontrolle

Die Tabelle beschreibt alle möglichen Werte und Standardwerte aller Einstellungen, die Sie für die Aufgabe zur Programmkontrolle angeben können.

Einstellungen der Aufgabe zur Programmkontrolle

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 Programmkategorie, 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.

Parameter	Description	Werte
`IncludeFileNames.item_#`	Der Name einer ausführbaren Datei, der die Regel auslöst	Bei der Angabe von Dateinamen können Sie **Masken** verwenden. Sie können das Zeichen * (beliebige Zeichenfolge) oder das Zeichen ? (beliebiges einzelnes Zeichen) verwenden, um eine Maske für einen Datei- oder Verzeichnisnamen zu bilden. Sie können das Zeichen * verwenden, um eine beliebige Anzahl an Zeichen (auch null Zeichen) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/*/file*/` oder `/dir/file*/`. Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.
`IncludeFolders.item_#`	Der Name eines Verzeichnisses mit einer ausführbaren Anwendungsdatei, welche die Regel auslöst	Bei der Angabe von Verzeichnisnamen können Sie **Masken** verwenden. Sie können das Zeichen * (beliebige Zeichenfolge) oder das Zeichen ? (beliebiges einzelnes Zeichen) verwenden, um eine Maske für einen Datei- oder Verzeichnisnamen zu bilden. Sie können das Zeichen * verwenden, um eine beliebige Anzahl an Zeichen (auch null Zeichen) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/*/file*/` oder `/dir/file*/`. Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.
`IncludeHashes.item_#`	SHA256-Hash einer ausführbaren Datei, der die Regel auslöst	Es ist nur SHA256 zulässig.
`UseExcludes`	Verwendung von Ausschlussbedingungen, um die Regel auszulösen	`Yes` – Regel nicht auf eine 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. Sie können das Zeichen * (beliebige Zeichenfolge) oder das Zeichen ? (beliebiges einzelnes Zeichen) verwenden, um eine Maske für einen Datei- oder Verzeichnisnamen zu bilden. Sie können das Zeichen * verwenden, um eine beliebige Anzahl an Zeichen (auch null Zeichen) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/*/file*/` oder `/dir/file*/`. Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.
`ExcludeFolders.item_#`	Der Name eines Verzeichnisses mit einer ausführbaren Anwendungsdatei, welche die Regel auslöst	Bei der Angabe von Verzeichnisnamen können Sie **Masken** verwenden. Sie können das Zeichen * (beliebige Zeichenfolge) oder das Zeichen ? (beliebiges einzelnes Zeichen) verwenden, um eine Maske für einen Datei- oder Verzeichnisnamen zu bilden. Sie können das Zeichen * verwenden, um eine beliebige Anzahl an Zeichen (auch null Zeichen) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/*/file*/` oder `/dir/file*/`. Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.
`ExcludeHashes.item_#`	SHA256-Hash einer ausführbaren Datei, der die Regel auslöst	Es ist nur SHA256 zulässig.

Parameter	Description	Werte
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.
`Kategorie`	Der Name der Programmkategorie, 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`	Gibt einen Benutzer oder eine Benutzergruppe an, für welche die Regel für die Programmkontrolle gelten soll.	`\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.
`Kategorie`	Der Name der erstellten Programmkategorie, 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.
`Principal`	Gibt einen Benutzer oder eine Benutzergruppe an, für welche die Regel für die Programmkontrolle gelten soll.	`\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.

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 <Pfad zur Konfigurationsdatei>
```

wobei:

`--file <Pfad zur Konfigurationsdatei>` ist der Pfad zur Konfigurationsdatei mit den Kategorieeinstellungen.

Die Datei mit den Kategorieeinstellungen sollte die folgende Struktur haben:

```
[
    {
        "Exclude" : [ "(FilePath like <vollständiger Pfad zur ausführbaren Datei des
   Programms>)", "(FileHash == <Hash der ausführbaren Datei>)" ],
        "GUID" : "<eindeutige ID der Kategorie>",
        "Include" : [ "(FilePath like <vollständiger Pfad zur ausführbaren Datei des
   Programms>)", "(FileHash == <Hash der ausführbaren Datei>)" ],
        "Name" : "<Kategoriename 1>"
    },
  {
        "Exclude" : [ "(FilePath like <vollständiger Pfad zur ausführbaren Datei des
   Programms>)", "(FileHash == <Hash der ausführbaren Datei>)" ],
        "GUID" : "<eindeutige ID der Kategorie>",
        "Include" : [ "(FilePath like <vollständiger Pfad zur ausführbaren Datei des
   Programms>)", "(FileHash == <Hash der ausführbaren Datei>)" ],
        "Name" : "<Kategoriename 2>"
    }
]
```

Zur Angabe des Dateinamens in den Feldern `Exclude` und `Include` können Sie **Masken** verwenden.

Sie können das Zeichen * (beliebige Zeichenfolge) oder das Zeichen ? (beliebiges einzelnes Zeichen) verwenden, um eine Maske für einen Datei- oder Verzeichnisnamen zu bilden.

Sie können das Zeichen * verwenden, um eine beliebige Anzahl an Zeichen (auch null Zeichen) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens / zu ersetzen. Beispiel: `/dir/*/file*/` oder `/dir/file*/`.

Sie können das Symbol ? eines einzelnen Zeichens (einschließlich des Symbols `/`) in einem Datei- oder Verzeichnisnamen verwenden.

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 Programmkategorien zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-categories [--names <Kategoriename 1> <Kategoriename 2> …
<Kategoriename N>] --file <Pfad zur Konfigurationsdatei>
```

wobei:

- `<Kategoriename 1> <Kategoriename 2> … <Kategoriename N>` sind die Namen der Kategorien, deren Informationen Sie ändern möchten. Wenn Sie Informationen mehrerer Kategorien ändern möchten, geben Sie die Kategorienamen durch ein Leerzeichen getrennt an. Wenn Sie keinen Kategorienamen angeben, werden vorhandene Kategorien gelöscht und neue Kategorien aus der angegebenen Datei erstellt.
- `--file <Pfad zur Konfigurationsdatei>` ist der Pfad zur Konfigurationsdatei mit den Kategorieeinstellungen.

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 <Pfad zur Konfigurationsdatei>] [--json]
```

wobei:

- `--file <Pfad zur Konfigurationsdatei>` ist der vollständige Pfad zur JSON-Konfigurationsdatei, in die die Einstellungen geschrieben werden.
- `--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie das Argument "--json" nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Kaspersky Endpoint Security zeigt folgende Informationen zu jeder 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 <Name der Kategorie 1> <Name der Kategorie 2>
... <Name der Kategorie N>] [--file <Pfad zur Konfigurationsdatei>] [--json]
```

wobei:

- `<Name der Kategorie 1> <Name der Kategorie 2> ... <Name der Kategorie N>` sind die Namen der Kategorien, zu denen Sie Informationen anzeigen möchten. Wenn Sie Informationen mehrerer Kategorien anzeigen möchten, geben Sie die Kategorienamen durch ein Leerzeichen getrennt an.
- `--file <Pfad zur Konfigurationsdatei>` – vollständiger Pfad zur JSON-Konfigurationsdatei, in die die Kategorieliste exportiert wird.
- `--json` – Gibt die Einstellungen im JSON-Format aus. Wenn Sie das Argument "--json" nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Wenn Sie in den Einstellungen der Aufgabe zur App-Kontrolle im Abschnitt `[Categories.item_#]` zum Einschließen oder Ausschließen von Bedingungen für das Auslösen einer Regel symbolische Links zur App-Datei oder zu einem Verzeichnis mit einer ausführbaren Datei angegeben haben, dann wird beim Anzeigen der Liste der App-Kategorien für diese Bedingungen der Quellpfad angezeigt, auf den der symbolische Link verweist.

Einstellung der Liste mit Regeln für die Programmkontrolle

Um eine Liste mit den Regeln der Programmkontrolle anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-settings 21 [--file <Pfad zur Konfigurationsdatei>] [--json]
```

wobei:

- `--file <Pfad zur Konfigurationsdatei>` 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 Programmkontrolle gilt.

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 <Pfad zur Konfigurationsdatei>] [--json]
```

wobei:

- `--file <Pfad zur Konfigurationsdatei>` 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 Programmkategorien und den Regeln der Programmkontrolle zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 21 --set-to-default
```

Parameter der Programmkontrolle exportieren und importieren

Um die Konfiguration der Komponente "Programmkontrolle" auf den Benutzergeräten zu vereinfachen, können Sie Parameter der Programmkontrolle und eine Liste von Programmkategorien exportieren und importieren.

Export und Import der Parameter der Programmkontrolle in der Web Console

In der Web Console können Sie die Einstellungen der Programmkontrolle sowie eine Liste der Programmkategorien in den Eigenschaften eines verwalteten Geräts exportieren und importieren (**Assets (Geräte)** → **Verwaltete Geräte** → Link <Name des Geräts> → **Regist**erkarte Anwendung → Link **<Name der Anwendung "Ka**spersky Endpo**int Security">** → Registerkarte Anwendungseinstellungen → Abschnitt Programmkontrolle).

Durch das Anklicken der Schaltfläche **Exportieren** im Block **Einstellungen der Programmkontrolle** wird ein Fenster geöffnet, in dem Sie die Datei angeben können, in der die konfigurierten Parameter gespeichert werden sollen. Durch das Anklicken der Schaltfläche **Importieren** im Block **Einstellungen der Programmkontrolle** wird ein Fenster geöffnet, in dem Sie die Datei angeben können, aus der die Parameter importiert werden sollen.

Durch das Anklicken der Schaltfläche **Exportieren** im Block **Programmkategorien** wird ein Fenster geöffnet, in dem Sie die Datei angeben können, in der die hinzugefügten Programmkategorien gespeichert werden sollen. Durch das Anklicken der Schaltfläche **Importieren** im Block **Programmkategorien** wird ein Fenster geöffnet, in dem Sie die Datei angeben können, aus der die Programmkategorien importiert werden sollen.

Export und Import der Parameter der Programmkontrolle in der Verwaltungskonsole

In der Verwaltungskonsole können Sie die Einstellungen der Programmkontrolle sowie eine Liste der Programmkategorien in den Eigenschaften eines verwalteten Geräts exportieren und importieren (**Verwaltete Geräte** → Registerkarte **Geräte** → Fenster mit den Geräteeigenschaften → Abschnitt **Anwendung** → <Name der Anwendung> → Schaltfläche **Eigenschaften** → Fenster **Parameter von <Name der Anwendung>** → Abschnitt **Programmkontrolle**).

Durch das Anklicken der Schaltfläche **Exportieren** im Block **Einstellungen der Programmkontrolle** wird ein Fenster geöffnet, in dem Sie die Datei angeben können, in der die konfigurierten Parameter gespeichert werden sollen. Durch das Anklicken der Schaltfläche **Importieren** im Block **Einstellungen der Programmkontrolle** wird ein Fenster geöffnet, in dem Sie die Datei angeben können, aus der die Parameter importiert werden sollen.

Durch das Anklicken der Schaltfläche **Exportieren** im Block **Programmkategorien** wird ein Fenster geöffnet, in dem Sie die Datei angeben können, in der die hinzugefügten Programmkategorien gespeichert werden sollen. Durch das Anklicken der Schaltfläche **Importieren** im Block **Programmkategorien** wird ein Fenster geöffnet, in dem Sie die Datei angeben können, aus der die Programmkategorien importiert werden sollen.

Export und Import der Parameter der Programmkontrolle über die Befehlszeile

Über die Befehlszeile können Sie die Parameter der Programmkontrolle und eine Liste der Programmkategorien mithilfe der Befehle zur Verwaltung der Programmkontrolle exportieren und importieren.

Inventarisierung

Mithilfe der Aufgabe Inventarisierung erhalten Sie Informationen über alle ausführbaren Dateien der Anwendung, die auf den Client-Geräten gespeichert sind. Das Abrufen von Informationen über die Anwendungen, die auf den Geräten installiert sind, kann sinnvoll sein, um z. B. Regeln für die Programmkontrolle zu erstellen.

Um die Aufgabe nutzen zu können, benötigen Sie eine Lizenz, in der diese Funktionalität enthalten ist.

Sie können die folgenden Einstellungen der Inventarisierung konfigurieren:

- Wählen Sie die Objekttypen aus, welche die Anwendung während der Inventarisierung auf dem Gerät erkennen soll (Dateien, Skripte).
- Konfigurieren Sie Inventarisierungsbereiche (Pfade zu Verzeichnissen, in denen nach ausführbaren Anwendungsdateien gesucht werden soll).
- Konfigurieren Sie Ausschlüsse von der Inventarisierung.
- Legen Sie Aktion fest, die Kaspersky Endpoint Security mit der Programmkategorie "Golden Image" nach Abschluss der Inventarisierungsaufgabe ausführt: Sie können der Kategorie Anwendungen hinzufügen, die durch die Ausführung der Aufgabe auf dem Gerät gefunden wurden, oder die Kategorie unverändert lassen oder löschen.
- Aktivieren oder deaktivieren Sie das Übertragen von Informationen über Anwendungen, die beim Ausführen der Inventarisierungsaufgabe auf dem Gerät erkannt wurden, an den Administrationsserver von Kaspersky Security Center. Wenn Informationen über Anwendungen auf dem Gerät an den Administrationsserver übertragen werden, können diese verwendet werden, um mittels Kaspersky Security Center Programmkategorien zu konfigurieren, auf deren Grundlage die Regeln der Komponente Programmkontrolle erstellt werden.

Inventarisierung in der Web Console konfigurieren

In der Web Console 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 Inventarisierungseinstellungen konfigurieren, indem Sie die Einstellungen für diese Aufgaben ändern.

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 Aufgabe "Inventarisierung" mit der Programmkategorie "Golden Image" ausführt: • **Ohne Änderungen belassen** – Nach Abschluss der Inventarisierung wird die Programmkategorie "Golden Image" nicht geändert. Dieser Wert ist standardmäßig ausgewählt. • **Aktualisieren oder erstellen (wenn nicht erstellt)** – Fügt die von der Aufgabe "Inventarisierung" auf dem Gerät gefundenen Anwendungen zur Programmkategorie "Golden Image" hinzu. Wenn die Kategorie nicht existiert, wird sie erstellt. Wenn eine Kategorie existiert, wird die Liste der darin enthaltenen Anwendungen aktualisiert. • **Löschen** – Nach Abschluss der Inventarisierung wird die Programmkategorie "Golden Image" gelöscht. Sie können die Kategorie "Golden Image" in 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	Eine Tabelle mit Inventarisierungsbereichen, die von der Anwendung untersucht werden sollen. Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle einen einzigen Inventarisierungsbereich: /usr/bin. Sie können Inventarisierungsbereiche in der Tabelle hinzufügen, ändern, löschen, nach oben verschieben und nach unten verschieben. Sie können auch eine Liste mit Inventarisierungsbereichen aus einer Datei importieren, indem Sie auf die Schaltfläche **Importieren** klicken und die Liste der Inventarisierungsbereiche über die Schaltflächen **Exportieren** in eine Datei im JSON-Format exportieren. Beim Importieren wird Ihnen vorgeschlagen, entweder die Liste der Inventarisierungsbereiche zu ersetzen oder die Inventarisierungsbereiche zu einer bestehenden Liste hinzuzufügen.

Fenster zum Hinzufügen des Untersuchungsbereichs

In diesem Fenster können Sie einen Untersuchungsbereich für die Inventarisierungsaufgabe hinzufügen und bearbeiten.

Einstellungen des Inventarisierungsbereichs

Parameter	Description
Name des Bereichs	Eingabefeld für den Namen des Inventarisierungsbereichs. Dieser Name wird in der Tabelle im Abschnitt **Untersuchungseinstellungen** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung des Bereichs während der Ausführung der Aufgabe. Wenn das Kontrollkästchen aktiviert ist, verarbeitet die Anwendung diesen Inventarisierungsbereich während der Ausführung der Aufgabe. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die Anwendung diesen Inventarisierungsbereich 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.

Parameter	Description
Dateisystem, Zugriffsprotokoll und Pfad	Eingabefeld für den Pfad des lokalen Verzeichnisses, das in den Inventarisierungsbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld darf nicht leer sein. Standardmäßige Pfadangabe **/** – Die Anwendung untersucht alle Verzeichnisse des lokalen Dateisystems.
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.

Abschnitt "Ausschlussbereiche"

Im Abschnitt **Ausschlussbereiche** können Sie für die Inventarisierungsaufgabe Ausschlussbereiche für die Untersuchung konfigurieren.

Fenster "Ausschlussbereiche"

Das Fenster enthält die Ausschlussbereiche einer Untersuchung. Die Anwendung untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden.

Einstellungen des Ausschlussbereichs

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 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 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.

Fenster zum Hinzufügen des Ausschlussbereichs

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 Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld darf nicht leer sein.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der Anwendung von der Untersuchung ausgeschlossen werden. Sie können Masken hinzufügen, bearbeiten und löschen.

Inventarisierung in der Verwaltungskonsole konfigurieren

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 konfigurieren, indem Sie die Aufgabeneinstellungen ändern.

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 Aufgabe "Inventarisierung" mit der Programmkategorie "Golden Image" ausführt: • **Ohne Änderungen belassen** – Nach Abschluss der Inventarisierung wird die Programmkategorie "Golden Image" nicht geändert. Dieser Wert ist standardmäßig ausgewählt. • **Aktualisieren oder erstellen (wenn nicht erstellt)** – Fügt die von der Aufgabe "Inventarisierung" auf dem Gerät gefundenen Anwendungen zur Programmkategorie "Golden Image" hinzu. Wenn die Kategorie nicht existiert, wird sie erstellt. Wenn eine Kategorie existiert, wird die Liste der darin enthaltenen Anwendungen aktualisiert. • **Löschen** – Nach Abschluss der Inventarisierung wird die Programmkategorie "Golden Image" gelöscht. Sie können die Kategorie "Golden Image" in 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 Anwendung diesen Untersuchungsbereich während der Ausführung der Aufgabe. Wenn das Kontrollkästchen deaktiviert ist, verarbeitet die Anwendung 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 Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld darf nicht leer sein.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der Anwendung während der Ausführung der Aufgabe untersucht werden. Standardmäßig enthält die Liste die Maske ***** (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen.

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 Anwendung untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden.

Einstellungen des Ausschlussbereichs

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 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 Sie **Masken** verwenden. Das Feld darf nicht leer sein. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der Anwendung von der Untersuchung ausgeschlossen werden. Sie können Masken hinzufügen, bearbeiten und löschen.

Inventarisierung über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie eine Inventarisierung der Anwendungen auf dem geschützten Gerät auf folgende Arten durchführen:

- Mithilfe der vordefinierten Aufgabe Inventarisierung (*Inventory_Scan*). Sie können diese Aufgabe manuell starten und beenden und den Zeitplan für den Aufgabenstart konfigurieren. Sie können die Einstellungen für die Untersuchung konfigurieren, indem Sie die Einstellungen für diese Aufgabe ändern.

- Mithilfe von Benutzeraufgaben zur Inventarisierung (Aufgaben vom Typ *InventoryScan*). Sie können Benutzeraufgaben manuell starten, beenden, anhalten und fortsetzen und den Zeitplan für den Aufgabenstart konfigurieren.

Sie können die Liste der Anwendungen, die auf einem Gerät als Ergebnis der Ausführung der Inventarisierungsaufgabe erkannt wurden, mithilfe der Befehle zur Verwaltung der Programmkontrolle anzeigen.

Einstellungen der Inventarisierungsaufgabe

Die Tabelle beschreibt alle möglichen Werte sowie die Standardwerte aller Einstellungen, die Sie für die Inventarisierungsaufgabe 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).	`Ja` (Standardwert) – Binärdateien untersuchen. `No` – Binärdateien nicht untersuchen.
`ScanAllExecutable`	Aktiviert die Untersuchung von Dateien mit Executable Bit.	`Ja` (Standardwert) – Dateien mit Executable Bit untersuchen. `No` – Dateien mit Executable Bit nicht untersuchen.
`GoldenImageAction`	Aktion, die Kaspersky Endpoint Security mit der Programmkategorie "Golden Image" nach Abschluss der Inventarisierungsaufgabe ausführt: Sie können die Kategorie "Golden Image" in Regeln der Programmkontrolle verwenden.	`DoNothing` (Standardwert) – Nach Abschluss der Inventarisierung wird die Programmkategorie "Golden Image" nicht geändert. `Create` – Erkannte Anwendungen werden zur Programmkategorie "Golden Image" hinzufügt. Wenn die Kategorie nicht existiert, wird sie erstellt. Wenn eine Kategorie existiert, wird die Liste der darin enthaltenen Anwendungen aktualisiert. `Remove` – Nach Abschluss der Inventarisierung wird die Programmkategorie "Golden Image" entfernt.
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.	Standardwert: `All objects`
`UseScanArea`	Aktiviert die Untersuchung des angegebenen Inventarisierungsbereichs. Um die Aufgabe auszuführen, müssen Sie mindestens einen Inventarisierungsbereich angeben.	`Yes` (Standardwert) – Den angegebenen Inventarisierungsbereich untersuchen. `No` – Den angegebenen Inventarisierungsbereich nicht untersuchen.

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 Anwendung 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 Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Liste der gefundenen Anwendungen 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 Anwendungen 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 Anwendungen mit folgenden Informationen:
  - **Pfad**. Pfad zur Anwendung.
  - **Hash**. Hash-Summe der Anwendung.
  - **Typ**. Typ der Anwendung. Zum Beispiel: `Script`, `Executable`.
  - **Kategorie**. Kategorien, zu denen die Anwendung gehört (falls sie zuvor erstellt wurden). Sie können die Liste der erstellten Programmkategorien mit dem Befehl `kesl-control --get-categories` anzeigen.

Wenn Sie eine neue Kategorie hinzufügen, werden deren Informationen in der Liste der Anwendungen nicht automatisch aktualisiert. Um die Liste der Anwendungen zu aktualisieren, müssen Sie die Inventarisierungsaufgabe neu starten.

Gerätekontrolle

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

Die Komponente "Gerätekontrolle" wird beim Start von Kaspersky Endpoint Security automatisch mit den Standardeinstellungen aktiviert.

Die Gerätekontrolle verwaltet den Zugriff auf den folgenden Ebenen:

- **Gerätetyp** gemäß der Klassifizierung der Komponente "Gerätekontrolle" (z. B. Drucker, Wechseldatenträger, CD-/DVD-Laufwerke). Für jeden Gerätetyp kann einer der folgenden Zugriffsmodi verwendet werden:
  - *Erlauben* – Gewährt Zugriff auf Geräte dieses Typs.
  - *Blockieren*: 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.
  - *Nach Regeln* – Zugriff auf Geräte erlauben oder blockieren, abhängig von den Regeln für den Zugriff auf Geräte. *Gerätezugriffsregel* – Eine Reihe von Einstellungen, die bestimmen, welche Benutzer zu welcher Zeit auf Geräte zugreifen können, die auf dem Client-Gerät installiert oder daran angeschlossen sind. 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.
  - *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 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.
- **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.

Standardmäßig ist für alle Gerätetypen der Zugriffsmodus *Abhängig vom Verbindungsbus* ausgewählt. Für Verbindungsbusse ist der Zugriffsmodus *Erlauben* ausgewählt. Basierend auf diesen Einstellungen gewährt die Gerätekontrolle Benutzern vollen Zugriff auf alle Geräte.

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.

Wenn die Komponente "Gerätekontrolle" beendet wird, entsperrt die Anwendung den Zugriff auf gesperrte Geräte.

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.

Sie können die Gerätekontrolle aktivieren und deaktivieren sowie die folgenden Ausführungseinstellungen der Komponente konfigurieren:

- Auswählen des Ausführungsmodus der Anwendung, beim Versuch, auf ein Gerät zuzugreifen, auf das der Zugriff gemäß den Einstellungen der Gerätekontrolle verboten ist: Blockieren oder nur über einen Zugriffsversuch auf das Gerät informieren.
- Auswählen des Zugriffsmodus für Geräte je nach ihrem Typ.
- Auswählen des Zugriffsmodus auf die Geräte in Abhängigkeit der Schnittstelle, über welche die Geräte angeschlossen sind.
- Ausschließen einzelner Geräte aus dem Aktionsbereich der Gerätekontrolle, indem Sie diese zur Liste der vertrauenswürdigen Geräte hinzufügen. *Vertrauenswürdige Geräte* – Geräte, auf die Benutzer vollen Zugriff haben. Sie können 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. Darüber hinaus können Sie Benutzer oder Benutzergruppen angeben, für welche die Geräte als vertrauenswürdig gelten.

  Sie können die Liste der vertrauenswürdigen Geräte über die Befehlszeile oder mithilfe von Kaspersky Security Center verwalten.

  Sie können Geräte nach ID oder Geräte-ID-Maske zur Liste der vertrauenswürdigen Geräte hinzufügen. Sie können Informationen über Geräte, die auf Client-Geräten installiert oder mit ihnen verbunden wurden, mittels der Befehlszeile auf dem Client-Gerät oder über Kaspersky Security Center abrufen. Die Übertragung von Informationen zum Administrationsserver von Kaspersky Security Center ist standardmäßig aktiviert.

  > Informationen zu Geräten werden nur übertragen, wenn ein Client-Gerät durch eine aktive Richtlinie verwaltet wird und eine Synchronisierung mit dem Administrationsagenten stattgefunden hat (wird in dem Intervall ausgeführt, das in den Eigenschaften der Richtlinie des Administrationsagenten festgelegt ist – standardmäßig alle 15 Minuten).

Wenn Sie die Anwendung über Kaspersky Security Center verwalten, können Sie auch Folgendes verwenden, um Geräte zur Liste der vertrauenswürdigen Geräte hinzuzufügen:

- Liste der Geräte, die auf verwalteten Client-Geräten erkannt wurden. Die Liste wird in den Richtlinieneigenschaften in der Web Console oder in der Verwaltungskonsole angezeigt.
- Liste der Geräte, die auf Basis der Ereignisse der Gerätekontrolle von Kaspersky Security Center erstellt wurde. Sie können diese Liste in den Richtlinieneigenschaften der Verwaltungskonsole erstellen.

In der Verwaltungskonsole können Sie außerdem die konfigurierte Liste der vertrauenswürdigen Geräte in eine Datei exportieren und eine Liste mit Geräten aus einer Datei importieren.

- Konfiguration des Zugriffszeitplans für Geräte, die für das Speichern von Daten vorgesehen sind (Festplatten, Wechseldatenträger, Disketten, CD/DVD-Laufwerke).

  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.

- Konfigurieren von Zugriffsregeln für Geräte je nach ihrem Typ. Sie können bestimmten Benutzern zu bestimmten Zeiten den Zugriff erlauben oder verweigern.
- Benutzern das Anfordern von temporärem Zugriff auf ein blockiertes Gerät erlauben und ihnen Zugriff auf das blockierte Gerät gewähren.

  Das Gewähren von Zugriff auf ein blockiertes Gerät ist nur dann verfügbar, wenn in der Organisation die Anwendung "Kaspersky Security Center 16.2" bereitgestellt ist und das Client-Gerät eine Verbindung mit dem Administrationsserver herstellen kann.

Gerätekontrolle in der Web Console konfigurieren

In der Web Console können Sie Einstellungen der Gerätekontrolle in den Richtlinieneigenschaften konfigurieren (**Anwendungseinstellungen** → **Sicherheitskontrolle** → **Gerätekontrolle**).

Gerätekontrolle in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen der Gerätekontrolle in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Sicherheitskontrolle** → **Gerätekontrolle.**) verwalten.

Einstellungen der Komponente "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.

Parameter	Description
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	Bei aktiviertem Kontrollkästchen kann der Benutzer in der grafischen Oberfläche oder in der Befehlszeile der Anwendung temporären Zugriff auf ein blockiertes 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.

Parameter	Description
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.
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

Parameter	Description
Typ	**Benutzer** oder **Gruppe**, für welchen bzw. welche die Regel 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 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.

Benachrichtigungsvorlagen der Gerätekontrolle konfigurieren

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 Fenster **Richtlinieneigenschaften → Sicherheitskontrolle → Gerätekontrolle**.
2. Klicken Sie im Block **Benachrichtigungsvorlagen** auf den Link **Nachricht bei blockiertem Gerät**.

3. Konfigurieren Sie im neuen Fenster **Benachrichtigungsvorlagen** auf der Registerkarte **Benachrichtigung an den Benutzer** die Benachrichtigungsvorlage der Gerätekontrolle.

   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**.

   Sie können außerdem den ursprünglichen Text der Benachrichtigungsvorlage wiederherstellen, indem Sie auf die Schaltfläche **Standardtext wiederherstellen** klicken.

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

5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

So passen Sie eine Benachrichtigungsvorlage in der Verwaltungskonsole an:

1. Öffnen Sie in der Struktur der Verwaltungskonsole im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu der die erforderlichen Geräte gehören.

2. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.

3. Wählen Sie in der Liste der Richtlinien die erforderliche Richtlinie aus und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>** mit einem Doppelklick.

   Sie können das Fenster mit den Richtlinieneigenschaften auch über den Eintrag **Eigenschaften** im Kontextmenü der Richtlinie oder durch Klicken auf den Link **Richtlinieneinstellungen konfigurieren** rechts neben der Liste der Richtlinien im Block mit den Richtlinieneinstellungen öffnen.

4. Wählen Sie im Fenster der Richtlinie die Option **Sicherheitskontrolle → 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**.

Gerätekontrolle über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Gerätekontrolle mithilfe der vordefinierten Aufgabe "Gerätekontrolle" (*Device_Control*) verwalten.

Die Aufgabe zur Gerätekontrolle wird standardmäßig nicht gestartet. Sie können diese Aufgabe manuell starten und anhalten.

Sie können die Einstellungen der Gerätekontrolle konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zur Gerätekontrolle ändern.

Mithilfe der Befehle zur Verwaltung der Gerätekontrolle können Sie außerdem die:

- Liste der verbundenen Geräte anzeigen und in eine Datei exportieren
- Liste der vertrauenswürdigen Geräte anzeigen und ändern

Einstellungen der Gerätekontrolle

Die Tabelle beschreibt alle möglichen Werte sowie die Standardwerte aller Einstellungen, die Sie für die Aufgabe Gerätekontrolle angeben können.

Einstellungen der Gerätekontrolle

Parameter	Description	Werte
`OperationMode`	Ausführungsmodus der Anwendung 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` – Erlaubt dem Benutzer, in der grafischen Oberfläche oder in der Befehlszeile der Anwendung temporären Zugriff auf ein blockiertes 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.

Parameter	Description	Werte
`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.
`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.

Parameter	Description	Werte
`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.
`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.

Parameter	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` Geben Sie im Abschnitt `[TrustedDevices.item_#] DeviceId=<Geräte-ID>` an *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*`
`Kommentar`	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. `<Benutzername>` 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>\<Benutzername>` oder `<Benutzername>@<Domänenname>`). `@<Gruppenname>` 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.	Standardwert: `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 `Standard`- Zeitplan kann nicht gelöscht werden.

Parameter	Description	Werte

DaysHours	Gibt die Zeitintervalle für einen Zeitplan an.	All (Standardwert) – Der Zeitplan gilt für 24/7 (keine zeitliche Begrenzung).
		
		< Wochentag > ist der Tag der Woche. 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.
		
		< Stunde > ist die Stunde [0:24]. Als Stunden können Sie nur Intervalle angeben.
		
		Beispiele:
		So legen Sie den Zeitplan "schedule_1" fest, der die Tage von Sonntag bis Samstag von 0 bis 11, von 12 bis 15 und von 16 bis 24 abdeckt:
		`[Schedules.item_0001]`
		`ScheduleName=schedule_1`
		`DaysHours=Su-Sa:0..11,12..15,16..24`
		So legen Sie den Zeitplan "schedule_2" fest, der die folgenden Intervalle abdeckt: Donnerstag von 12 bis 14, Freitag von 2 bis 15 und von 16 bis 24:
		`[Schedules.item_0002]`
		`ScheduleName=schedule_2`
		`DaysHours=Th:12..14;Fr:2..15,16..24`
		So legen Sie den Zeitplan "schedule_3" fest, der 24 Stunden und 7 Tage die Woche abdeckt:
		`[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.	Die Zugriffsregel \Everyone (Standardwert) gilt für alle Benutzer. < Benutzername > ist der Name eines lokalen Benutzers oder Domänenbenutzers, für den die Zugriffsregel gilt (ohne den vollständigen Namen mit Domäne anzugeben, wenn das System die Eingabe von Benutzernamen in diesem Format zulässt, oder im Format <Domänenname>\<Benutzername> oder <Benutzername>@<Domänenname>). @< Gruppenname > ist der Name der (lokalen oder Domänen-)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.	Standardwert: 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.		

Parameter	Description	Werte
Principal	Gibt einen Benutzer oder eine Benutzergruppe an, für welche die Zugriffsregel gelten soll.	Die Zugriffsregel \Everyone (Standardwert) gilt für alle Benutzer. < Benutzername > ist der Name eines lokalen Benutzers oder Domänenbenutzers, für den die Zugriffsregel gilt (ohne den vollständigen Namen mit Domäne anzugeben, wenn das System die Eingabe von Benutzernamen in diesem Format zulässt, oder im Format <Domänenname>\<Benutzername> oder <Benutzername>@<Domänenname>). @< Gruppenname > ist der Name der (lokalen oder Domänen-)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.	Standardwert: Default.
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.	Die Zugriffsregel \Everyone (Standardwert) gilt für alle Benutzer. < Benutzername > ist der Name eines lokalen Benutzers oder Domänenbenutzers, für den die Zugriffsregel gilt (ohne den vollständigen Namen mit Domäne anzugeben, wenn das System die Eingabe von Benutzernamen in diesem Format zulässt, oder im Format <Domänenname>\<Benutzername> oder <Benutzername>@<Domänenname>). @< Gruppenname > ist der Name der (lokalen oder Domänen-)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.	Standardwert: 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.	Die Zugriffsregel \Everyone (Standardwert) gilt für alle Benutzer. < Benutzername > ist der Name eines lokalen Benutzers oder Domänenbenutzers, für den die Zugriffsregel gilt (ohne den vollständigen Namen mit Domäne anzugeben, wenn das System die Eingabe von Benutzernamen in diesem Format zulässt, oder im Format <Domänenname>\<Benutzername> oder <Benutzername>@<Domänenname>). @< Gruppenname > ist der Name der (lokalen oder Domänen-)Benutzergruppe, für die die Zugriffsregel gilt.

Parameter	Description	Werte
`[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.	Standardwert: `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.

Liste der verbundenen Geräte in der Befehlszeile anzeigen und exportieren

Um eine Liste mit den verbundenen Geräten anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --get-device-list [--all] [--json]
```

wobei:

- `--all` – Gibt eine Liste aller verbundenen Geräte aus.
- `--json` – Gibt eine Liste aller verbundenen Geräte im JSON-Format aus.

Kaspersky Endpoint Security zeigt folgende Informationen zu den angeschlossenen Geräten an:

- **Gerätetyp**. Der Typ des angeschlossenen Geräts. Zum Beispiel `OpticalDrive` oder `HardDrive`.
- **ID (Kennung)**. ID des angeschlossenen Geräts.
- **Name**. Name des angeschlossenen Geräts.
- **Pfad**. Pfad des Gerätes im virtuellen Betriebssystem sysfs.
- **Systemlaufwerk**. Diese Einstellung gibt an, ob das angeschlossene Gerät ein Systemlaufwerk ist (ja oder nein).
- **Bus**. Verbindungsbus. Mögliche Werte: `UnknownBus`, `USB`, `FireWire`.
- **Treiber**. Der Name des zu verwendenden Treibers, wie er vom virtuellen Betriebssystem sysfs gelesen wird.

Um eine Liste der verbundenen Geräte zu exportieren, führen Sie den folgenden Befehl aus:

```
kesl-control --get-device-list --export <Datei>
```

wobei `<Datei>` der vollständige Pfad zur JSON-Datei ist, in der Sie die Liste der verbundenen Geräte speichern möchten.

Der Export erfolgt als Liste vertrauenswürdiger Geräte.

Liste vertrauenswürdiger Geräte über die Befehlszeile verwalten

Die Liste der vertrauenswürdigen Geräte enthält Informationen über Geräte, für welche der Zugriff gewährt wurde (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.

Um eine Liste mit den vertrauenswürdigen Geräten anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control --trusted-devices --list
```

Um ein Gerät zur Liste der vertrauenswürdigen Geräte hinzuzufügen, führen Sie den folgenden Befehl aus:

```
kesl-control --trusted-devices --add <ID>
```

wobei `<ID>` der Geräte-ID oder einer Maske der Geräte-ID entspricht.

Um ein Gerät aus der Liste der vertrauenswürdigen Geräte zu entfernen, führen Sie den folgenden Befehl aus:

```
kesl-control --trusted-devices --delete <ID>
```

wobei `<ID>` der Geräte-ID oder einer Maske der Geräte-ID entspricht.

Um eine Liste mit vertrauenswürdigen Geräten aus einer Datei zu importieren, führen Sie den folgenden Befehl aus:

```
kesl-control --trusted-devices --merge|--add|--replace --file <Datei>
```

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 <Datei>` ist der vollständige Pfad zur JSON-Datei, aus der die Liste der vertrauenswürdigen Geräte importiert wird.

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 der Web Console, der Verwaltungskonsole oder in den Einstellungen der 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 in der grafischen Oberfläche oder in der Befehlszeile der Anwendung den temporären Zugriff auf ein blockiertes Gerät 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. Das Gewähren des Zugriffs auf das gesperrte Gerät erfolgt in der Web Console.

3. Der Benutzer lädt den Zugriffsschlüssel hoch und erhält temporären Zugriff auf das gesperrte Gerät. Der Zugriffsschlüssel kann über die grafische Benutzeroberfläche oder die Befehlszeile der Anwendung hochgeladen werden.

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.

Zugriff auf ein Gerät in der Web Console gewähren

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.

Wenn der Administrator von einem Benutzer eine Anfrage auf temporären Zugriff erhält, kann er in der Web Console aus der Datei mit der Zugriffsanfrage einen Zugriffsschlüssel erstellen.

Um temporären Zugriff auf ein Gerät zu gewähren, benötigt der Administrator die Lese-, Schreib- und Ausführungsberechtigungen für die **Funktion zur Datenverschlüsselung** (**Benutzer und Rollen** → **Rollen** → <Benutzerrolle> → Fenster mit den Eigenschaften der Benutzerrolle → Registerkarte **Zugriffsberechtigungen** → <Name der Anwendung> → **Datenverschlüsselung** → **Lesen/Schreiben/Ausführen**).

So erstellen Sie einen Zugriffsschlüssel für ein gesperrtes 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.

Temporären Zugriff auf ein Gerät über die Befehlszeile erhalten

Wenn ein Benutzer der Meinung ist, das der Zugriff auf ein Gerät oder die Vorgänge mit den Geräteinhalten irrtümlich gesperrt wurden, kann der Benutzer beim Administrator des lokalen Netzwerks der Organisation temporären Zugriff auf das gesperrte Gerät anfordern, indem er den folgenden Befehl zur Verwaltung der Gerätekontrolle ausführt: `kesl-control --request-temporary-device-access`.

Um temporären Zugriff auf ein gesperrtes Gerät anzufordern, führen Sie folgenden Befehl aus:

```
kesl-control --request-temporary-device-access --device-id <Geräte-ID> --access-duration <Zugriffsdauer> --path <Pfad zur Datei mit der Zugriffsanfrage>
```

wobei:

`--device-id <Geräte-ID>` – ID des gesperrten Geräts, auf das Sie zugreifen möchten.

`--access-duration <Dauer des Zugriffs>` – Dauer des Intervalls, für welches Sie Zugriff auf das Gerät bekommen möchten (in Stunden). Mögliche Werte: 1 – 100.

`--path <Pfad zur Zugriffsanfrage-Datei>` – Pfad zum Verzeichnis, in dem Sie die Zugriffsanfrage-Datei mit key-Erweiterung 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).

Wenn der Zugriffsschlüssel vom Administrator erhalten wurde, muss der Zugriffsschlüssel mittels des Befehls `kesl-control --upload-temporary-device-access-key` hochgeladen werden, um temporären Zugriff zu bekommen.

Um temporären Zugriff auf ein gesperrtes Gerät zu erhalten, führen Sie folgenden Befehl aus:

```
kesl-control --upload-temporary-device-access-key --path <Pfad zur Datei mit Zugriffsschlüssel>
```

wobei:

`--path <Pfad zur Datei mit Zugriffsschlüssel>` – Pfad zur Datei mit dem Zugriffsschlüssel für das Gerät (Datei mit acode-Erweiterung).

Der Befehl zeigt Informationen über die dem Gerät gewährten Zugriffsrechte und den Zeitraum an, für den diese Zugriffsrechte gelten.

Web-Kontrolle

Die Web-Kontrolle steuert den Benutzerzugriff 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 den Besuch der Website nicht empfiehlt.

Kaspersky Endpoint Security überwacht nur HTTP- und HTTPS-Datenverkehr.

Mit der Web-Kontrolle können Sie den Zugriff auf Seiten anhand folgender Methoden konfigurieren:

- Nach Inhaltskategorien. Die Kategorisierung des Inhalts von Seiten erfolgt mittels des Cloud-Dienstes Kaspersky Security Network, durch heuristische Analyse und anhand einer Datenbank bekannter Seiten (diese ist Teil der Anwendungsdatenbank). Sie können beispielsweise den Benutzerzugriff auf die Inhaltskategorie "Soziale Netzwerke" oder auf andere Kategorien beschränken.

- Nach Datentypkategorien. Sie können den Benutzerzugriff nach Datenarten auf der Seite einschränken und beispielsweise Grafiken ausblenden. Die Anwendung bestimmt den Datentyp anhand des Dateiformats, nicht anhand der Erweiterung.

  Die Anwendung untersucht keine Dateien in Archiven. Wenn beispielsweise Bilddateien archiviert werden, erkennt die Anwendung den Datentyp als "Archive" und nicht als "Bilddateien".

- Nach Webadresse. Sie können eine Adresse oder eine Maske für Adressen angeben.

Sie können mehrere Methoden verwenden, um den Zugriff auf Seiten gleichzeitig zu steuern. Beispielsweise können Sie den Zugriff auf die Datentypkategorie "Dateien von Office-Anwendungen" für die Inhaltskategorie "Web-Mail" beschränken.

Standardmäßig ist für alle Webressourcen die *Standardregel* **Erlauben** ausgewählt. Gemäß dieser Regel erlaubt die Web-Kontrolle den Benutzern den Zugriff auf Webressourcen, sofern keine anderen *Regeln für den Zugriff auf Webressourcen* angegeben sind.

Sie können die Standardregel für die Web-Kontrolle, nach der die Anwendung den Zugriff auf Webressourcen reguliert, die nicht durch andere Regeln abgedeckt sind, ändern, und die Standardregel **Blockieren** *festlegen*. Gemäß dieser Regel verbietet die Web-Kontrolle den Benutzern den Zugriff auf Webressourcen, sofern keine anderen *Regeln für den Zugriff auf Webressourcen* angegeben sind.

Wenn Sie Ausnahmen vom Abfangen des Datenverkehrs mittels Kaspersky Endpoint Security konfiguriert haben, wirken sich diese auf die Funktion der Komponente "Web-Kontrolle" aus.

Über die Zugriffsregeln für Webressourcen

Eine Zugriffsregel auf Webressourcen besteht aus einer Reihe von Filtern und einer Aktion, die von der Anwendung angewendet werden, wenn ein Benutzer die in der Regel beschriebenen Webressourcen zu dem im Zeitplan der Regel angegebenen Zeitpunkt besucht. Mithilfe von Filtern können Sie Webressourcen angeben, auf die der Zugriff durch die Komponente "Web-Kontrolle" kontrolliert wird.

Es stehen folgende Filter zur Verfügung:

- **Filter nach Inhaltskategorien** Die Web-Kontrolle kann Webressourcen in Inhaltskategorien aufteilen. Sie können den Benutzerzugriff auf Webressourcen kontrollieren, die durch diese Kategorien definierte Inhalte enthalten. Wenn ein Benutzer eine Webressource besucht, die zu der ausgewählten Inhaltskategorie gehört, führt die Anwendung die in der Regel angegebene Aktion aus.

- **Filter nach Datentypkategorien**. Die Web-Kontrolle kann Webressourcen nach Datentypkategorien aufteilen. Sie können den Benutzerzugriff auf bestimmte Arten von Daten kontrollieren, die als Webressourcen veröffentlicht werden. Wenn ein Benutzer eine Webressource abruft, die zur ausgewählten Datentypkategorie gehört, führt die Anwendung die in der Regel angegebene Aktion aus.

- **Filter nach Adressen der Webressourcen**. Sie können den Benutzerzugriff auf alle Adressen einer Webressource, auf einzelne Adressen einer Webressource und/oder für Adressgruppen einer Webressource kontrollieren.

  Wenn sowohl ein Filter nach Inhaltskategorien und/oder Datentypkategorien als auch ein Filter nach Adressen der Webressourcen angegeben ist und die angegebenen Adressen bzw. Adressgruppen der Webressourcen zu den ausgewählten Inhaltskategorien oder Datentypkategorien gehören, kontrolliert die Anwendung den Zugriff nicht auf alle Webressourcen der ausgewählten Inhaltskategorien und/oder Datentypkategorien, sondern nur auf die angegebenen Adressen bzw. Adressgruppen von Webressourcen.

- **Filter nach Benutzername und Benutzergruppe**. Sie können Benutzer und/oder Benutzergruppen angeben, für die der Zugriff auf Webressourcen gemäß der Regel gesteuert wird. Sie können beispielsweise den Internetzugriff über einen Browser für alle Unternehmensmitarbeiter beschränken, aber die IT-Abteilung ausnehmen.

- **Anwendungszeitplan der Regel**. Sie können für die Regel einen Anwendungszeitplan festlegen. Der Anwendungszeitplan der Regeln bestimmt den Zeitpunkt, an dem die Anwendung den Zugriff auf die in der Regel angegebenen Webressourcen kontrolliert. Sie können beispielsweise den Internetzugriff über einen Browser nur während der Arbeitszeit beschränken.

Für jede Regel können Sie die Aktion angeben, die von der Web-Kontrolle ausgeführt wird, wenn ein Benutzer eine Webressource besucht, die den Einstellungen in der Regel entspricht:

- *Erlauben.* Die Web-Kontrolle erlaubt den Benutzerzugriff auf Webressource.

- *Blockieren.* Die Web-Kontrolle verweigert den Benutzerzugriff auf Webressource und zeigt eine Meldung über die Zugriffsverweigerung an. Durch Klicken auf die Links in der Blockierungsmeldung kann der Benutzer eine Beschwerdemeldung über die irrtümliche Blockierung an den Administrator des lokalen Netzwerks der Organisation senden und Zugriff auf die blockierte Webressource anfordern.

- *Informieren.* Die Web-Kontrolle zeigt eine Warnung an, dass es nicht empfohlen wird, die Webressource zu besuchen. Durch Klicken auf die Links in der Warnmeldung kann der Benutzer eine Beschwerdemeldung über die irrtümliche Warnung an den Administrator des lokalen Netzwerks der Organisation senden. Dabei wird der Zugriff des Benutzers auf die Webressource nicht blockiert.

Jede Regel besitzt eine Priorität. Je höher sich eine Regel in der Liste befindet, desto höher ist ihre Priorität. Wenn eine Seite mehreren Regeln hinzugefügt wird, regelt die Web-Kontrolle den Zugriff auf diese Seite entsprechend der Regel mit der höchsten Priorität. Beispielsweise könnte die Anwendung das Web-Portal eines Unternehmens als soziales Netzwerk definieren. Um den Zugriff auf soziale Netzwerke einzuschränken, ohne dabei den Zugriff auf das Web-Portal des Unternehmens zu verlieren, müssen Sie zwei Regeln erstellen: eine Verbotsregel für die Inhaltskategorie "Soziale Netzwerke" und eine Erlaubnisregel für das Web-Portal des Unternehmens. Die Zugriffsregel für das Web-Portal des Unternehmens sollte dabei eine höhere Priorität bekommen als die Zugriffsregel für soziale Netzwerke.

Wenn gar keine Verbotsregel erstellt wurde, wird der HTTPS-Verkehr nicht entschlüsselt.

Die Web-Kontrolle in der Web Console konfigurieren

In der Web Console können Sie die Einstellungen der Web-Kontrolle in den Richtlinieneigenschaften konfigurieren (**App-Einstellungen** → **Sicherheitskontrolle** → **Web-Kontrolle**).

Die Web-Kontrolle in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen der Web-Kontrolle in den Richtlinieneigenschaften verwalten (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Sicherheitskontrolle** → **Web-Kontrolle**).

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**.
	Ein Klick auf die Schaltfläche **Nach unten** bewegt das ausgewählte Element in der Tabelle nach unten.
	Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.
	Ein Klick auf die Schaltfläche **Nach oben** bewegt das ausgewählte Element in der Tabelle nach oben.
	Diese Schaltfläche ist verfügbar, wenn in der Tabelle mindestens ein Element ausgewählt ist.
	Sie können auch eine Liste mit Regeln aus einer Datei importieren, indem Sie auf die Schaltfläche **Erweitert** -> **Importieren** klicken und die Liste der hinzugefügten Regeln über die Schaltflächen **Erweitert** -> **Ausgewählte exportieren** oder **Erweitert** -> **Alle exportieren** in eine Datei exportieren. Beim Importieren wird Ihnen vorgeschlagen, entweder die Liste mit Regeln zu ersetzen oder die Regeln zu einer bestehenden Liste hinzuzufügen.

Standard-Regel	In der Dropdown-Liste können Sie eine Standardregel, nach der die 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.

Der Web-Kontrolle eine Regel hinzufügen

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.

Parameter	Description
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.

Benachrichtigungsvorlagen der Web-Kontrolle konfigurieren

Abhängig von der Aktion, die in den Eigenschaften der Regel für die Web-Kontrolle angegeben ist, zeigt die Anwendung beim Zugriffsversuch eines Benutzers auf Webressourcen eine Nachricht an (die Antwort des HTTP-Servers wird durch eine HTML-Seite mit einer Nachricht ersetzt), der folgenden Typen entsprechen kann:

- Warnmeldung. Diese Meldung warnt den Benutzer, dass der Besuch der Webressource nicht empfohlen wird und/oder nicht den Sicherheitsrichtlinien des Unternehmens entspricht. Die Anwendung zeigt eine Warnmeldung an, wenn in den Einstellungen der Regel für diese Webressource die Aktion **Informieren** ausgewählt ist.

  Sollte die Warnung nach Ansicht des Benutzers irrtümlich angezeigt werden, kann der Benutzer über einen in der Warnmeldung enthaltenen Link eine bereits vorformulierte Anfrage an den Administrator des lokalen Netzwerks der Organisation senden.

- Nachricht über blockierte Webressource Die App zeigt eine Meldung an, dass die Webressource blockiert wurde, wenn in den Einstellungen der Regel, die dieser Webressource entspricht, die Aktion **Blockieren** ausgewählt ist.

  Sollte die Blockierung des Zugriffs auf die Webressource nach Ansicht des Benutzers irrtümlich geschehen sein, kann der Benutzer über einen in der Nachricht enthaltenen Link eine bereits vorformulierte Anfrage an den Administrator des lokalen Netzwerks der Organisation senden.

Für die Warnmeldung, die Nachricht über das Blockieren des Zugriffs auf eine Webressource und die Anfrage an den Administrator des lokalen Netzwerks der Organisation sind bereits erstellte Vorlagen verfügbar. Sie können deren Inhalt anpassen.

So bearbeiten Sie die Nachrichtenvorlage in der Web Console:

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

   Die Liste mit Richtlinien wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, welche die Geräte enthält, auf jene die Richtlinie angewendet wird. Klicken Sie dazu auf den Link im Feld "Aktueller Pfad" oben im Fenster und wählen Sie im angezeigten Fenster die Administrationsgruppe aus.

   In der Liste werden die Richtlinien angezeigt, die für die ausgewählte Administrationsgruppe konfiguriert sind.

3. Klicken Sie in der Liste auf den Namen der erforderlichen Richtlinie.

   Das Eigenschaftenfenster der Richtlinie wird geöffnet.

4. Wählen Sie im Eigenschaftsfenster der Richtlinie die Option **Anwendungseinstellungen** → **Security Controls** → **Web Control** aus.

5. Konfigurieren Sie im Block **Vorlagen für Nachrichten** die Benachrichtigungsvorlagen der Web-Kontrolle auf den folgenden Registerkarten:

   - **Warnung**. Das Eingabefeld enthält eine Benachrichtigungsvorlage, die beim Auslösen einer Regel angezeigt wird und vor einem Versuch warnt, auf eine nicht empfohlene Webressource zuzugreifen.

   - **Nachricht beim Blockieren**. Das Eingabefeld enthält eine Vorlage für die Meldung, die erscheint, wenn eine Regel ausgelöst wird, die den Zugriff auf eine Webressource blockiert.

   - **Nachricht an den Administrator**. Das Eingabefeld enthält eine Vorlage für eine Anfrage, die an den Administrator des lokalen Netzwerks der Organisation gesendet werden kann, wenn nach Meinung des Benutzers der Zugriff auf die Webressource irrtümlich blockiert wurde. Nachdem ein Benutzer die Gewährung des Zugriffs beantragt hat, sendet Kaspersky Endpoint Security das Ereignis *Nachricht an den Administrator über den verweigerten Zugriff auf ein Webseiten* an Kaspersky Security Center. Die Ereignisbeschreibung enthält eine an den Administrator gerichtete Nachricht mit ersetzten Variablen. Wenn Kaspersky Security Center in Ihrer Organisation nicht verwendet wird oder keine Verbindung zum Administrationsserver besteht, sendet die Anwendung eine Nachricht an die angegebene E-Mail-Adresse des Administrators.

   Auf den Registerkarten **Warnung und Nachricht beim Blockieren** können Sie Variablen und Links zu den Nachrichten für den Benutzer hinzufügen, indem Sie auf die Schaltflächen **Variable hinzufügen** und **Link hinzufügen** klicken.

   Sie können den ursprünglichen Text der Nachrichtenvorlage wiederherstellen, indem Sie auf die Schaltfläche **Zurücksetzen** klicken.

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

7. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

So passen Sie eine Benachrichtigungsvorlage in der Verwaltungskonsole an:

1. Öffnen Sie in der Struktur der Verwaltungskonsole im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu der die erforderlichen Geräte gehören.

2. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.

3. Wählen Sie in der Liste der Richtlinien die erforderliche Richtlinie aus und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>** mit einem Doppelklick.

   Sie können das Fenster mit den Richtlinieneigenschaften auch über den Eintrag **Eigenschaften** im Kontextmenü der Richtlinie oder durch Klicken auf den Link **Richtlinieneinstellungen konfigurieren** rechts neben der Liste der Richtlinien im Block mit den Richtlinieneinstellungen öffnen.

4. Wählen Sie im Fenster der Richtlinie die Option **Sicherheitskontrolle → Web-Kontrolle** aus.

5. Klicken Sie im 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**.

Die Web-Kontrolle über die Befehlszeile konfigurieren

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 diese Aufgabe manuell starten und anhalten.

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.

Einstellungen der Aufgabe "Web-Kontrolle"

Die untere Tabelle beschreibt alle verfügbaren Werte und Standardwerte aller Einstellungen, die Sie für die Aufgabe zur Web-Kontrolle angeben können.

Einstellungen der Aufgabe "Web-Kontrolle"

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.	`Keine` (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, GenerativeAITools`

`[Rules.item_#.FormatCategories.item_#]`	Abschnitt zur Angabe der Datentypkategorien.	–
`FormatCategories.item_#.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.	`< Benutzername >` ist der Name des Benutzers, für den die Regel gilt. `@< Gruppenname >` 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` `0` -ID des Zeitplans `Default` (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.	`< Wochentag >` ist der Tag der Woche. 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. `< Stunde >` ist die Stunde [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 < Pfad zur Konfigurationsdatei >] [--json]
```

wobei:

`--file < Pfad zur Konfigurationsdatei >` ist der vollständige Pfad zur Konfigurationsdatei, in die die Einstellungen geschrieben werden.

`--json` – Gibt Daten im JSON-Format aus.

Um die Einstellungen der Web-Kontrolle zu ändern, führen Sie den folgenden Befehl aus:

```
kesl-control --set-settings 26 [--file < Pfad zur Konfigurationsdatei >] [--json]
```

wobei:

`--file < Pfad zur Konfigurationsdatei >` ist der vollständige Pfad zur Konfigurationsdatei, aus der die Einstellungen importiert werden.

`--json` – Importiert die Daten aus einer Datei im JSON-Format importiert.

Führen Sie den folgenden Befehl aus, um die konfigurierten Einstellungen zu löschen und die Werte für die Einstellungen der Web-Kontrolle auf die Standardregel zurückzusetzen:

```
kesl-control --set-settings 26 --set-to-default
```

Regeln zum Definieren von Adressmasken für Webressourcen

Die Verwendung einer *Adressmasken für eine Webressource* (im Weiteren auch "Adressmaske") kann in praktisch sein, wenn Sie beim Erstellen einer Zugriffsregel für Webressourcen viele ähnlich lautende Adressen von Webressourcen eingeben müssen. So kann eine entsprechend formulierte Adressmaske viele Adressen von Webressourcen ersetzen.

Beim Erstellen einer Adressmaske sollten folgende Regeln beachtet werden:

1. Das `*`-Zeichen ersetzt eine beliebige Sequenz von null oder mehr Zeichen.

   Wenn Sie beispielsweise die Adressmaske `*abc*` eingeben, wird die Zugriffsregel der Webressourcen auf alle Adressen angewendet, in denen die Sequenz `abc` enthalten ist. Beispiel: `http://www.example.com/page_0-9abcdef.html`.

2. Die Zeichenfolge `*.` ermöglicht die Auswahl aller Domänen einer Adresse und stellt damit eine *Domänenmaske* dar. Die Domänenmaske `*.` wird als beliebiger Domänenname, Subdomänenname oder leere Zeichenfolge behandelt.

   Beispiel: Die folgenden Adressen unterliegen der Maske `*.example.com`:

   - `http://pictures.example.com` – die Domänenmaske `*.` entspricht `pictures.`.
   - `http://user.pictures.example.com` – wobei die Domänenmaske `*.` auf `pictures` und `user` angewendet wird.
   - `http://example.com` – wobei die Domänenmaske `*.` als leere Zeichenfolge behandelt wird.

3. Die Sequenz `www.` am Anfang einer Adressmaske wird als Sequenz `*` interpretiert..

   Beispiel: Die Adressmaske `www.example.com` wird als `*.example.com` interpretiert. Die Maske deckt auch die Adressen `www2.example.com` und `www.pictures.example.com` ab.

4. Wenn eine Adressmaske nicht mit dem Zeichen `*` beginnt, entspricht der Inhalt der Adressmaske demselben Inhalt mit dem Präfix `*.`.

5. Wenn eine Adressmaske mit einem anderen Zeichen als `/` oder `*` endet, entspricht der Inhalt der Adressmaske demselben Inhalt mit dem Postfix `/*`.

   Beispiel: Die Adressmaske `http://www.example.com` deckt die Adressen der Form `http://www.example.com/abc` ab, wobei `a`, `b`, `c` beliebige Zeichen sein können.

6. Wenn eine Adressmaske mit einem `/`-Zeichen endet, entspricht der Inhalt der Adressmaske demselben Inhalt mit dem Postfix `/*`.

7. Die Zeichenfolge `/*` am Ende der Adressmaske wird als `/*` oder als leere Zeichenfolge behandelt.

8. Die Prüfung der Adressen von Webressourcen nach Adressmasken erfolgt unter Berücksichtigung des Schemas (http oder https):

   - Wenn in der Adressmaske kein Netzwerkprotokoll angegeben ist, fällt eine Adresse mit einem beliebigen Netzwerkprotokoll unter die Adressmaske.

     Beispiel: Die Adressmaske `example.com` deckt die Adressen `http://example.com` und `https://example.com` ab.

   - Wenn in der Adressmaske ein Netzwerkprotokoll angegeben ist, werden von der Adressmaske nur Adressen mit demselben Netzwerkprotokoll, wie es in der Adressmaske enthalten ist, abgedeckt.

     Beispiel: Die Adressmaske `http://*.example.com` deckt die Adresse `http://www.example.com` ab, aber nicht die Adresse `https://www.example.com`.

9. Eine mit doppelten Anführungszeichen umschlossene Adressmaske wird ohne Berücksichtigung weiterer Ersetzungen behandelt, mit Ausnahme des `*`-Zeichens, wenn es ursprünglich in der Adressmaske enthalten war. Für Adressmasken, die von doppelten Anführungszeichen umschlossen sind, werden die Regeln 5 und 7 nicht angewendet (siehe Beispiele 14 – 18 in der unteren Tabelle).

10. Beim Vergleich mit einer Adressmaske für Webressourcen werden Benutzername, Passwort und Verbindungsport sowie die Groß- und Kleinschreibung nicht berücksichtigt.

Beispiele zur Anwendung der Regeln für die Erstellung von Adressmasken

Nr.	Adressmaske	Geprüfte Adresse einer Webressource	Entspricht die geprüfte Adresse der Adressmaske?	Kommentar
1	*.example.com	http://www.123example.com	Nein	Siehe Regel 1
2	*.example.com	http://www.123.example.com	Ja	Siehe Regel 2
3	*example.com	http://www.123example.com	Ja	Siehe Regel 1
4	*example.com	http://www.123.example.com	Ja	Siehe Regel 1
5	http://www.*.example.com	http://www.123example.com	Nein	Siehe Regel 1
6	www.example.com	http://www.example.com	Ja	Siehe Regeln 3, 2, 1
7	www.example.com	https://www.example.com	Ja	Siehe Regeln 3, 2, 1
8	http://www.*.example.com	http://123.example.com	Ja	Siehe Regeln 3, 4, 1
9	www.example.com	http://www.example.com/abc	Ja	Siehe Regeln 3, 5, 1
10	example.com	http://www.example.com	Ja	Siehe Regeln 3, 1
11	http://example.com/	http://example.com/abc	Ja	Siehe Regel 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.

Überwachung der System-Integrität

Mit Kaspersky Endpoint Security können Sie die Integrität des Betriebssystems des geschützten Geräts in Echtzeit und auf Befehl überwachen.

- Mit der Komponente *Überwachung der Systemintegrität* können Sie Änderungen in Dateien und Verzeichnissen, die Sie in den Komponenteneinstellungen in den Überwachungsbereich aufgenommen haben, in Echtzeit überwachen. Sie können Änderungen an Dateien überwachen, die eventuell auf eine Verletzung der Sicherheit auf dem geschützten Gerät hindeuten.

- Mithilfe von Aufgaben zur *Prüfung der Systemintegrität* können Sie Dateien und Verzeichnisse, die Sie in den Überwachungsbereich aufgenommen haben, auf Änderungen überprüfen, indem Sie den aktuellen Status des überwachten Objekts mit einem zuvor erfassten Status vergleichen.

Um die Überwachung der Systemintegrität nutzen zu können, benötigen Sie eine Lizenz, in der diese Funktionalität enthalten ist.

Wenn Kaspersky Endpoint Security im Überwachungsbereich Änderungen an Dateien und Verzeichnissen erkennt, generiert es Ereignisse über Änderungen an den Listen zur Objektzugriffskontrolle. Die Komponente "Überwachung der Systemintegrität" übermittelt keine Informationen darüber, welche Änderungen genau vorgenommen wurden. Die Aufgabe *Prüfung der Systemintegrität* übermittelt Informationen über geänderte Attribute sowie verschobene Dateien und Verzeichnisse.

Überwachung der Systemintegrität in Echtzeit

Mit der Komponente "Überwachung der Systemintegrität" wird jede Änderung an einem Objekt im Überwachungsbereich registriert, indem Dateioperationen in Echtzeit abgefangen werden.

Während der Ausführung der Komponente "Überwachung der Systemintegrität" überwacht die Anwendung Änderungen der folgenden Dateieinstellungen:

- Inhalt (write (), truncate (), etc.)
- Metadaten (Besitzrechte (chmod/chown))
- Zeitstempel (utimensat)
- erweiterte Attribute (setxattr) und andere

Die Prüfsumme der Datei wird nicht berechnet.

Aufgrund der technischen Beschränkungen des Betriebssystems Linux kann die Anwendung nicht erkennen, welcher Benutzer oder Prozess die Änderungen an einer Datei durchgeführt hat.

Die Überwachung der System-Integrität ist standardmäßig deaktiviert. Sie können die Überwachung der Systemintegrität aktivieren und deaktivieren sowie die Ausführungseinstellungen der Komponente konfigurieren:

- Überwachungsbereiche für die Überwachung der Systemintegrität festlegen. Das Programm überwacht Dateioperationen in den Überwachungsbereichen, die in den Einstellungen der Überwachung der Systemintegrität definiert sind. Zur Ausführung der Komponente müssen Sie mindestens einen Überwachungsbereich angeben. Standardmäßig ist der Überwachungsbereich *Interne Objekte von Kaspersky* (/opt/kaspersky/kesl/) angegeben.

  Sie können mehrere Überwachungsbereiche angeben. Sie können den Überwachungsbereich im Echtzeitmodus ändern.

  > Die Anwendung führt keine Überwachung von Dateiänderungen (Attribute und Inhalt) mit harten Links durch, die sich nicht in einem Überwachungsbereich befinden.

- Sie können den Ausschluss von Objekten von der Überwachung anhand einer Namensmaske konfigurieren.

- Konfigurieren Sie Ausschlussbereiche zur Überwachung der Systemintegrität. Ausschlüsse werden für jeden einzelnen Überwachungsbereich angegeben und funktionieren nur für den angegebenen Bereich. Sie können mehrere Ausschlüsse vom Überwachungsbereich angeben.

  Ein Ausschluss hat eine höhere Priorität als der Überwachungsbereich; das ausgeschlossene Objekt wird nicht überwacht, auch wenn es sich im Überwachungsbereich befindet. Wenn ein Überwachungsbereich auf einer niedrigeren Ebene als dem im Ausschluss angegebenen Verzeichnis festgelegt ist, überwacht die Anwendung diesen Überwachungsbereich während der Überwachung der Systemintegrität nicht.

> Wenn ein Verzeichnis zum Überwachungs- oder Ausschlussbereich hinzugefügt wird, prüft die Anwendung nicht, ob das angegebene Verzeichnis existiert.

Überwachung der Systemintegrität in der Web Console konfigurieren

In der Web Console können Sie Einstellungen der Überwachung der Systemintegrität in den Richtlinieneigenschaften konfigurieren (**Anwendungseinstellungen** → **Sicherheitskontrolle** → **Überwachung der Systemintegrität**).

Überwachung der Systemintegrität in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen für die Überwachung der Systemintegrität in den Richtlinieneigenschaften (Verwalten von Richtlinien in der Verwaltungskonsole, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Sicherheitskontrolle** → **Überwachung der Systemintegrität**) verwalten.

Einstellungen der Komponente "Überwachung der Systemintegrität"

Parameter	Description
Überwachung der System-Integrität aktivieren	Dieses Kontrollkästchen aktiviert und deaktiviert die Überwachung der System-Integrität. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Überwachungsbereiche	Die Einstellungsgruppe enthält die Schaltfläche **Konfigurieren**. Durch Klicken auf diese Schaltfläche wird das Fenster **Untersuchungsbereiche** geöffnet.

Parameter	Description
Ausnahmen von der Überwachung	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.

Parameter	Description
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 Anwendung 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.

Parameter	Description
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.

Überwachung der Systemintegrität über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Überwachung der Systemintegrität in Echtzeit mithilfe der vordefinierten Aufgabe "Überwachung der Systemintegrität" (*System_Integrity_Monitoring*) verwalten. Aufgabentyp – *OAFIM*.

Die Aufgabe "Überwachung der Systemintegrität" wird standardmäßig nicht gestartet. Sie können diese Aufgabe manuell starten und anhalten.

Sie können die Einstellungen der Überwachung der Systemintegrität auf dem Gerät konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zur Überwachung der Systemintegrität ändern.

Einstellungen der Aufgabe zur Überwachung der 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 den Wert dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseExcludeMasks` aktiviert ist. Sie können mehrere Masken angeben. Jede Maske muss in einer neuen Zeile mit einem neuen Index angegeben werden.	Der Standardwert ist nicht angegeben.
Der Abschnitt **[ScanScope.item_#]** enthält die von der Aufgabe zur Überwachung der System-Integrität zu überwachenden Bereiche. Für die Aufgabe muss zumindest ein Überwachungsbereich festgelegt sein. Sie können mehrere Abschnitte [ScanScope.item_#] in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge. Der Abschnitt [ScanScope.item_#] enthält folgende Einstellungen:		
`AreaDesc`	Beschreibung des Überwachungsbereichs mit zusätzlichen Informationen über den Überwachungsbereich.	Der Standardwert ist nicht angegeben.
`UseScanArea`	Aktiviert die Überwachung des angegebenen Bereichs.	`Yes` (Standardwert) – Den angegebenen Bereich überwachen. `No` – Den angegebenen Bereich nicht überwachen.
`Path`	Pfad zum Verzeichnis, das überwacht werden soll.	Bei der Angabe des Pfades können Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardwert: /opt/kaspersky/kesl/
`AreaMask.item_#`	Einschränkung des Überwachungsbereichs. Im Überwachungsbereich untersucht die 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)

Parameter	Description	Werte
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 Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Der Standardwert ist nicht angegeben.
`AreaMask.item_#`	Einschränkung des Ausschlussbereichs von der Überwachung. Im Ausschlussbereich von der Überwachung schließt die 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)

Überwachung der System-Integrität

Während der Ausführung der Aufgabe *Prüfung der Systemintegrität* werden Änderungen in jedem Objekt ermittelt, indem der aktuelle Status des überwachten Objekts mit dem Originalstatus verglichen wird. Vergleiche können anhand der folgenden Kriterien durchgeführt werden:

- Hash-Summer der Datei
- Zeitpunkt der Dateiänderung
- Dateigröße

Der Originalstatus der überwachten Objekte wird als *Baseline* aufgezeichnet. Die Baseline enthält Pfade zu überwachten Objekten und deren Metadaten.

Die Baseline kann persönliche Daten enthalten.

Die Baseline wird während der ersten Ausführung der Aufgabe zur Prüfung der Systemintegrität auf dem Gerät erstellt. Wenn Sie mehrere Aufgaben zur Prüfung der Systemintegrität erstellt haben, wird für jede Aufgabe eine separate Baseline erstellt. Die Aufgabe wird nur ausgeführt, wenn die Baseline Informationen zu Objekten enthält, die zum für die Aufgabe konfigurierten Überwachungsbereich gehören. Wenn die Baseline nicht dem Überwachungsbereich entspricht, erstellt die Anwendung Kaspersky Endpoint Security ein Ereignis über die Verletzung der System-Integrität.

Die Baseline wird jedes Mal aktualisiert, wenn die Aufgabeneinstellungen geändert werden (z. B. wenn ein neuer Überwachungsbereich hinzugefügt wird), sowie wenn die Aufgabe mit der Einstellung `RebuildBaseline=Yes` gestartet wird (oder wenn in den Aufgabeneigenschaften in Kaspersky Security Center das Kontrollkästchen **Baseline bei jedem Aufgabenstart neu erstellen** aktiviert ist).

Die Anwendung erstellt Speicher für Baselines auf dem geschützten Gerät. Standardmäßig befindet sich der Speicher für Baselines unter /var/opt/kaspersky/kesl/private/fim.db. Für den Zugriff auf die Datenbank mit Baselines sind Root-Rechte erforderlich.

Sie können eine Baseline löschen, indem Sie die entsprechende Aufgabe zur Prüfung der Systemintegrität löschen.

Sie können die Prüfung der Systemintegrität auf Befehl durchführen und Einstellungen für die Prüfung konfigurieren:

- Aktivieren und deaktivieren Sie die Aktualisierung der Baseline jedes Mal nach Abschluss der Aufgabe zur Prüfung der Systemintegrität.
- Wählen Sie die Kriterien aus, anhand derer der aktuelle Status der überwachten Datei mit dem Originalstatus verglichen wird: Verwenden Sie den Hash und den Zeitpunkt der Dateiänderung oder nur die Dateigröße.
- Konfigurieren Sie Überwachungsbereiche zur Prüfung der Systemintegrität.
- Konfigurieren Sie Bereiche, die von der Prüfung der Systemintegrität ausgeschlossen werden sollen. Sie können Pfade zu ausgeschlossenen Dateien und Verzeichnissen angeben und einzelne Objekte anhand der Namensmaske ausschließen.

Prüfung der Systemintegrität in der Web Console

In der Web Console können Sie mithilfe der Aufgabe *Prüfung der Systemintegrität* Prüfungen der Systemintegrität durchführen.

Sie können Benutzeraufgaben für die Prüfung der Systemintegrität erstellen und starten. Sie können die Untersuchungseinstellungen konfigurieren, indem Sie die Aufgabeneinstellungen ändern.

Einstellungen der Aufgabe zur Untersuchung der System-Integrität

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 während der Prüfung der Systemintegrität. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Zeitpunkt des letzten Zugriffs auf Dateien überwachen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Überwachung des Zeitpunkts des Dateizugriffs während der Prüfung der Systemintegrität. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Überwachungsbereiche	Eine Tabelle mit Überwachungsbereichen, die von der Aufgabe untersucht werden sollen. Standardmäßig enthält die Tabelle den Überwachungsbereich **Interne Objekte von Kaspersky** (/opt/kaspersky/kesl/). Sie können Überwachungsbereiche in der Tabelle hinzufügen, ändern, löschen, nach oben verschieben und nach unten verschieben. Sie können auch eine Liste mit Überwachungsbereichen aus einer Datei importieren, indem Sie auf die Schaltfläche **Importieren** klicken und die Liste der Überwachungsbereiche über die Schaltflächen **Exportieren** in eine Datei im JSON-Format exportieren. Beim Importieren wird Ihnen vorgeschlagen, entweder die Liste der Überwachungsbereiche zu ersetzen oder die Überwachungsbereiche zu einer bestehenden Liste hinzuzufügen.

Fenster zum Hinzufügen des Untersuchungsbereichs

In diesem Fenster können Sie den Überwachungsbereich für die Aufgabe zur Überwachung der System-Integrität hinzufügen und bearbeiten.

Einstellungen des Überwachungsbereichs

Parameter	Description
Name des Bereichs	Eingabefeld für den Namen des Überwachungsbereichs. Dieser Name wird in der Tabelle im Abschnitt **Untersuchungseinstellungen** angezeigt. Das Eingabefeld darf nicht leer sein.
Diesen Bereich verwenden	Dieses Kontrollkästchen aktiviert und deaktiviert die Untersuchung dieses Bereichs während der Ausführung der 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.

Parameter	Description
Dateisystem, Zugriffsprotokoll und Pfad	Eingabefeld für den Pfad des lokalen Verzeichnisses, das in den Überwachungsbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld darf nicht leer sein. Standardmäßige Pfadangabe **/** – Die Anwendung untersucht alle Verzeichnisse des lokalen Dateisystems.
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.

Abschnitt "Ausschlussbereiche"

Im Abschnitt **Ausschlussbereiche** können Sie die Ausschlussbereiche von der Prüfung und Ausschlüsse nach Maske für die Aufgabe zur Überwachung der System-Integrität konfigurieren.

Fenster "Ausschlussbereiche"

Die Tabelle enthält die Ausschlussbereiche der Komponente "Prüfung der System-Integrität". Die App untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.

Einstellungen des Bereichs mit Ausschlüsse von der Überwachung

Parameter	Description
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 Überwachung ausschließt.

Die Elemente in der Tabelle können Sie hinzufügen, bearbeiten und löschen.

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.

Fenster zum Hinzufügen des Ausschlussbereichs

In diesem Fenster können Sie einen Bereich mit Ausschlüssen von der Überwachung für die Aufgabe zur Prüfung der System-Integrität hinzufügen und bearbeiten.

Einstellungen des Bereichs mit Ausschlüsse von der Überwachung

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 Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld darf nicht leer sein. Als Pfad ist standardmäßig **/** angegeben. Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der Anwendung von der Überwachung ausgeschlossen werden. Standardmäßig enthält die Liste die Maske ***** (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen.

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).

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

In der Verwaltungskonsole können Sie mithilfe der Aufgabe *Prüfung der Systemintegrität* Prüfungen der Systemintegrität durchführen.

Sie können Benutzeraufgaben für die Prüfung der Systemintegrität erstellen und starten. Sie können die Untersuchungseinstellungen konfigurieren, indem Sie die Aufgabeneinstellungen ändern.

Im Abschnitt **Einstellungen** in den Eigenschaften der Aufgabe "Prüfung der Systemintegrität" können Sie die in der folgenden Tabelle aufgeführten Einstellungen konfigurieren.

Einstellungen der Aufgabe zur Untersuchung der System-Integrität

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.

Im Abschnitt **Ausschlussbereiche** in den Eigenschaften der Aufgabe "Prüfung der Systemintegrität" können Sie Ausschlüsse vom Überwachungsbereich und Ausschlüsse nach Maske konfigurieren.

Fenster "Untersuchungsbereiche"

Die Tabelle enthält die Überwachungsbereiche der Aufgabe zur Prüfung der System-Integrität. Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle nur den Überwachungsbereich **Interne Kaspersky-Objekte** (/opt/kaspersky/kesl/).

Einstellungen des Überwachungsbereichs

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 Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld darf nicht leer sein. Standardmäßig ist der Pfad "/opt/kaspersky/kesl" angegeben.
Masken	Diese Liste enthält die Masken der Objektnamen, die von der Anwendung während ihrer Ausführung untersucht werden. Standardmäßig enthält die Liste die Maske ***** (alle Objekte). Sie können Masken hinzufügen, bearbeiten und löschen.

Abschnitt "Ausschlussbereiche"

Einstellungen der Ausnahmen von der Untersuchung

Einstellungsgruppe	Description
Ausnahmen von der Überwachung	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 Anwendung 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.

Parameter	Description
Dateisystem, Zugriffsprotokoll und Pfad	Eingabefeld für den Pfad des lokalen Verzeichnisses, das in den Ausschlussbereich aufgenommen werden soll. Bei der Angabe des Pfades können Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Feld darf nicht leer sein. Als Pfad ist standardmäßig **/** angegeben. Die App schließt alle Verzeichnisse des lokalen Dateisystems von der Untersuchung aus.
Masken	Diese Liste enthält die Namensmasken von Objekten, die von der 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).

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).

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 über die Befehlszeile konfigurieren

Sie können über die Befehlszeile eine Prüfung der Systemintegrität auf einem Gerät ausführen, indem Sie Benutzeraufgaben zur *Prüfung der Systemintegrität* (Aufgaben vom Typ *ODFIM*) verwenden.

Sie können Benutzeraufgaben manuell starten, beenden, anhalten und fortsetzen und den Zeitplan für den Aufgabenstart konfigurieren. Sie können die Einstellungen für die Prüfung der Systemintegrität konfigurieren, indem Sie die Einstellungen für diese Aufgaben ändern.

Einstellungen der Aufgabe zur Untersuchung der System-Integrität

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 Anwendung nur die Dateigröße (wenn sich die Dateigröße nicht geändert hat, wird der Zeitpunkt der Änderung nicht als kritischer Parameter betrachtet).
`TrackDirectoryChanges`	Aktiviert die Verzeichnisüberwachung.	`Yes` – Verzeichnisse während der Prüfung der Systemintegrität überwachen. `No` (Standardwert) – Verzeichnisse nicht überwachen.
`TrackLastAccessTime`	Aktiviert die Prüfung des Zeitpunkts des letzten Dateizugriffs In Linux-Betriebssystemen ist die der Parameter `noatime`.	`Yes` – Zeitpunkt des letzten Dateizugriffs prüfen. `No` (Standardwert) – Zeitpunkt des letzten Dateizugriffs nicht prüfen.
`UseExcludeMasks`	Aktiviert den Ausschluss von Objekten aus dem Überwachungsbereich, die in der Einstellung `ExcludeMasks.item_#` angegeben sind. Diese Einstellung funktioniert nur, wenn die Einstellung `ExcludeMasks.item_#` angegeben ist.	`Yes` – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, aus dem Überwachungsbereich ausschließen. `No` (Standardwert) – Objekte, die in der Einstellung `ExcludeMasks.item_#` angegeben sind, nicht aus dem Überwachungsbereich ausschließen.
`ExcludeMasks.item_#`	Ausschluss von der Überwachung von Objekten nach Name oder Maske. Mit dieser Einstellung können Sie eine einzelne Datei anhand des Namens oder mehrere Dateien anhand von Masken im Shell-Format aus dem angegebenen Untersuchungsbereich ausschließen. Bevor Sie den Wert dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UseExcludeMasks` aktiviert ist. Sie können mehrere Masken angeben. Jede Maske muss in einer neuen Zeile mit einem neuen Index angegeben werden.	Der Standardwert ist nicht angegeben.
Der Abschnitt **[ScanScope.item_#]** enthält die von der Aufgabe *Prüfung der Systemintegrität* zu überwachenden Bereiche. Für die Aufgabe muss zumindest ein Überwachungsbereich festgelegt sein. Sie können mehrere Abschnitte [ScanScope.item_#] in beliebiger Reihenfolge angeben. Die App verarbeitet die Elemente nach ihrem Index in aufsteigender Reihenfolge. Der Abschnitt [ScanScope.item_#] enthält folgende Einstellungen:		
`AreaDesc`	Beschreibung des Überwachungsbereichs mit zusätzlichen Informationen über den Überwachungsbereich.	Der Standardwert ist nicht angegeben.

Parameter	Description	Werte
`UseScanArea`	Aktiviert die Überwachung des angegebenen Bereichs.	`Yes` (Standardwert) – Den angegebenen Bereich überwachen. `No` – Den angegebenen Bereich nicht überwachen.
`Path`	Pfad zum Verzeichnis, das überwacht werden soll.	Bei der Angabe des Pfades können Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Standardwert: /opt/kaspersky/kesl/
`AreaMask.item_#`	Einschränkung des Überwachungsbereichs. Im Überwachungsbereich untersucht die 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.

Parameter	Description	Werte
`Path`	Pfad zum Verzeichnis mit Objekten, die von der Überwachung ausgeschlossen sind.	Bei der Angabe des Pfades können Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Der Standardwert ist nicht angegeben.
`AreaMask.item_#`	Einschränkung des Ausschlussbereichs von der Überwachung. Im Ausschlussbereich von der Überwachung schließt die 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)

Verhaltensanalyse

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

Die Komponente "Verhaltensanalyse" wird beim Start von Kaspersky Endpoint Security automatisch mit den Standardeinstellungen aktiviert.

Für eine optimale Leistung der Komponente „Verhaltensanalyse“ wird empfohlen, die Komponente Schutz vor Web-Bedrohungen zu aktivieren.

Sie können die Verhaltensanalyse aktivieren und deaktivieren sowie die Ausführungseinstellungen der Komponente konfigurieren, indem Sie:

- Wählen Sie die Aktion aus, die Kaspersky Endpoint Security ausführen soll, wenn im Betriebssystem schädliche Aktivitäten erkannt werden: Benutzer informieren oder Anwendung, die schädliche Aktivitäten ausführt, blockieren.
- Aktivitäten von Prozessen von der Untersuchung durch die Komponente "Verhaltensanalyse" und die Komponenten MDR und EDR Expert (on-premise) ausschließen.

  Die Anwendung schließt den Prozess des Watchdog-Servers automatisch von der Untersuchung aus. Diese Ausnahme kann nicht gelöscht werden.

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.

Wenn ein Benutzer mit root-Berechtigung keinen Zugriff auf eine Datei in einem über NFSv4 eingebundenen Remote-Verzeichnis hat, blockiert die Anwendung den Zugriff auf die Datei für alle Benutzer.

Verhaltensanalyse in der Web Console konfigurieren

In der Web Console können Sie die Einstellungen für die Verhaltensanalyse in den Richtlinieneigenschaften (**Programmeinstellungen** → **Host-Schutz** → **Verhaltensanalyse** → **Verhaltensanalyse**) verwalten.

Verhaltensanalyse in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen der Verhaltensanalyse in den Richtlinieneigenschaften verwalten (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**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 Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. Das Eingabefeld darf nicht leer sein.
Auf untergeordnete Prozesse anwenden	Untergeordnete Prozesse des 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 Anwendung diesen Bereich während ihrer Ausführung aus. Wenn das Kontrollkästchen deaktiviert ist, schließt die Anwendung 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.	Das Kontrollkästchen aktiviert oder deaktiviert das Ausschließen von Prozessaktivitäten aus den Telemetriedaten, die durch MDR und EDR Expert(on-premise) gesammelt werden. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Verhaltensanalyse über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Analyse des Verhaltens von Anwendungen im Betriebssystem mithilfe der vordefinierten Aufgabe "Verhaltensanalyse" (*Behavior_Detection*) verwalten.

Die Aufgabe "Verhaltensanalyse" wird standardmäßig ausgeführt. Sie können diese Aufgabe manuell starten und anhalten.

Sie können die Einstellungen für die Verhaltensanalyse konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zur Verhaltensanalyse ändern.

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 Anwendung 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.
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 Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.
`ApplyToDescendants`	Untergeordnete Prozesse des ausgeschlossenen Prozesses, der durch den `ProgramPath-` Parameter angegeben ist, von der Untersuchung ausschließen.	`Yes` – Schließt den angegebenen Prozess und alle seine untergeordneten Prozesse von der Untersuchung aus. `No` (Standardwert) – Nur den angegebenen Prozess von der Untersuchung ausschließen, untergeordnete Prozesse nicht von der Untersuchung ausschließen.
`ProgramDesc`	Beschreibung des ausgeschlossenen Prozesses.	
`UseTrustedProgram`	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.
`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.

Parameter	Description	Werte
`UseTrustedProgramForMDRAndEDR`	Wird verwendet, um Prozessaktivitäten aus den Telemetriedaten, die durch MDR und EDR Expert(on-premise) gesammelt werden, auszuschließend.	`Yes` – Schließt Prozessaktivitäten aus den Telemetriedaten, die durch MDR und EDR Expert(on-premise) gesammelt werden, aus. `No` (Standardwert) – Schließt keine Prozessaktivitäten aus den Telemetriedaten, die durch MDR und EDR Expert(on-premise) gesammelt werden, aus.
`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`		`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.

Exploit-Prävention

Die Komponente Exploit-Prävention überwacht Softwarecode, der Schwachstellen auf Ihrem Gerät ausnutzt, um Administratorrechte zu erlangen oder schädliche Vorgänge auszuführen. Exploits können beispielsweise einen Angriff mit Überlauf der Zwischenablage verwenden. Dazu sendet der Exploit große Datenvolumen an ein verwundbares Programm. Bei der Verarbeitung dieser Daten führt das verwundbare Programm schädlichen Code aus. Aufgrund dieses Angriffs kann der Exploit eine nicht autorisierte Installation von Schadsoftware starten. Wenn der Versuch, die ausführbare Datei einer Anwendung mit Schwachstelle auszuführen, nicht vom Benutzer ausgeht, blockiert Kaspersky Endpoint Security den Start dieser Datei oder informiert den Benutzer darüber. Standardmäßig ist die Exploit-Prävention deaktiviert.

Zur Ausführung der Komponente "Exploit-Prävention" muss die Komponente Verhaltensanalyse und die Verwendung des aktualisierbaren Kernel-Moduls aktiviert sein Für eine optimale Leistung der Komponente „Exploit-Prävention“ wird empfohlen, auch die Komponente Schutz vor Web-Bedrohungen zu aktivieren.

Sie können die Exploit-Prävention aktivieren und deaktivieren sowie die folgenden Ausführungseinstellungen der Komponente konfigurieren:

- Wählen Sie die Aktion aus, welche die Anwendung bei Erkennung eines Exploits ausführt.
- Konfigurieren Sie den Ausschluss von Objekten aus der Untersuchung. Eine Untersuchungsausnahme ist eine Reihe von Bedingungen. Wenn diese Bedingungen erfüllt sind, untersucht das Programm die Objekte nicht auf Viren und andere Malware. Sie können Folgendes von der Untersuchung ausschließen:
  - Objekte nach dem Namen der in den Objekten gefundenen Bedrohungen.
  - Dateien und Verzeichnisse, die sich an den angegebenen Pfaden befinden.
  - Dateien, welche eine angegebene Prüfsumme besitzen.

Exploit-Prävention in der Web Console konfigurieren

In der Web Console können Sie die Einstellungen für die Exploit-Prävention in den Eigenschaften der Richtlinie (**Programmeinstellungen** → **Host-Schutz** → **Verhaltensanalyse** → **Exploit-Prävention**) verwalten.

Exploit-Prävention in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen für die Exploit-Prävention in den Eigenschaften der Richtlinie verwalten (Verwalten von Richtlinien in der Verwaltungskonsole, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**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.
Block **Exploit-Prävention**	Über die Schaltfläche **Konfigurieren** öffnet sich das Fenster **Ausnahmen aus der Exploit-Prävention**, in dem Sie die Untersuchungsausnahmen der 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.
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.

Exploit-Prävention über die Befehlszeile konfigurieren

In der Befehlszeile können Sie die Exploit-Prävention mithilfe der Parameter der vordefinierten Aufgabe Verhaltensanalyse (*Behavior_Detection*) steuern.

Sie können die Einstellungen für die Exploit-Prävention konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe zur Verhaltensanalyse (siehe folgende Tabelle) ändern.

Einstellungen der Exploit-Prävention

Parameter	Description	Werte
`UseAEP`	Aktivieren der Komponente Exploit-Prävention.	`Ja` 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.	`Ja` (Standardwert) – die Ausnahme für die Exploit-Prävention verwenden. `No` – Verwendet keine Ausnahmen aus der Untersuchung der Exploit-Prävention.

Parameter	Description	Werte
`DetectName`	Schließt ein Objekt nach dem Namen der in im Objekt gefundenen Bedrohungen von der Untersuchung aus. Bevor Sie den Wert 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 den Wert dieser Einstellung festlegen, stellen Sie sicher, dass die Einstellung `UsePath` 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 einen Wert für diese 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, die die durch die Einstellung `DetectName` angegebenen Bedrohungen enthalten, 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.

Verwendung von Kaspersky Security Network

Die Funktionen für KSN sind in dieser Anwendung in den USA möglicherweise nicht verfügbar.

Für einen effektiveren Schutz von Geräten und Benutzerdaten kann Kaspersky Endpoint Security das Kaspersky Security Network (KSN) verwenden. KSN ist eine cloudbasierte Wissensdatenbank von Kaspersky mit Reputationen zu Dateien, Internetressourcen und Software. Die Verwendung der Daten aus Kaspersky Security Network gewährleistet eine schnellere Reaktion auf verschiedene Bedrohungen, eine hohe Leistung der Schutzkomponenten und eine Verringerung der Anzahl von Fehlalarmen.

Die Verwendung von Kaspersky Security Network ist freiwillig. Sie können die Verwendung von KSN jederzeit aktivieren oder deaktivieren.

Infrastrukturlösungen von Kaspersky Security Network

Kaspersky Endpoint Security unterstützt die folgenden Infrastrukturlösungen für die Verwendung der Reputationsdatenbanken von Kaspersky:

- *Kaspersky Security Network (KSN)* – Eine Lösung, mit der Sie Informationen von Kaspersky erhalten. Gleichzeitig senden Sie Daten über Objekte, die auf Benutzergeräten gefunden wurden, zur zusätzlichen Überprüfung an Kaspersky, wo sie von Kaspersky-Analysten und geprüft werden und zur Ergänzung in die Reputations- und Statistikdatenbanken eingehen.

- *Kaspersky Private Security Network (KPSN)* ist eine Lösung, die es Benutzern von Geräten mit installiertem Kaspersky Endpoint Security ermöglicht, auf die Reputationsdatenbanken und weitere statistische Daten von Kaspersky zuzugreifen, ohne dabei Daten von ihren Geräten an Kaspersky zu senden. KPSN ist für Unternehmenskunden konzipiert, die Kaspersky Security Network beispielsweise aus folgenden Gründen nicht nutzen können:

  - Lokale Arbeitsplätze haben keine Verbindung mit dem Internet.

  - Es gelten gesetzliche oder unternehmensinterne sicherheitsbezogene Einschränkungen, die es verbieten, Daten über die Grenzen des Landes oder des lokalen Netzwerks der Organisation hinaus zu senden.

Nachdem Sie die 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.

Möglichkeiten zur Verwendung von Kaspersky Security Network

Es gibt zwei Möglichkeiten, KSN zu verwenden:

- **Erweiterter KSN-Modus** – Erlaubt Ihnen das Abrufen von Informationen aus der Wissensdatenbank von Kaspersky, während Kaspersky Endpoint Security automatisch statistische Informationen an Kaspersky Security Network sendet, die im Rahmen seiner Ausführung entstehen. Ferner kann die Anwendung Dateien (oder Teile von Dateien), die von Angreifern zur Beschädigung des Geräts oder der Daten verwendet werden können, zur erweiterten Untersuchung an Kaspersky senden.

- **Standardmäßiger KSN-Modus** – Erlaubt Ihnen das Abrufen von Informationen aus der Wissensdatenbank von Kaspersky, während Kaspersky Endpoint Security keine anonymen Statistiken und Daten über Arten und Quellen von Bedrohungen sendet.

Sie können den Nutzungsmodus von Kaspersky Security Network über die Web Console, der Verwaltungskonsole oder die Befehlszeile auswählen.

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.

Cloud-Modus von Kaspersky Endpoint Security

Der *Cloud-Modus* ist ein Modus zur Ausführung von Kaspersky Endpoint Security, in dem die Anwendung eine schlankere Version der Malware-Datenbanken verwendet. Dies trägt dazu bei, die Auslastung des Gerätespeichers zu verringern.

Kaspersky Security Network unterstützt die Verwendung der schlanken Anti-Malware-Datenbanken durch das Programm.

Wenn Kaspersky Endpoint Security im Standard-Modus verwendet wird und Sie im Rahmen der Anwendungsausführung KSN verwenden, können Sie den Cloud-Modus der Anwendung aktivieren.

Wenn Sie Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwenden, wird die Verwendung der schlankeren Malware-Datenbanken nicht unterstützt. Die Anwendung erhält vom Schutzserver spezielle Datenbanken, die für den Betrieb des Light Agent erforderlich sind.

Kaspersky Endpoint Security wechselt zur Verwendung der schlankeren Version der Malware-Datenbanken, nachdem der Cloud-Modus aktiviert wurde und das nächsten Update der Datenbanken und Module der Anwendung durchgeführt wurde. Wenn der Cloud-Modus deaktiviert wird, lädt Kaspersky Endpoint Security beim nächsten Update die vollständige Version der Anwendungsdatenbanken von den Kaspersky-Servern herunter und aktualisiert die Datenbanken und Module der Anwendung.

Wenn Sie KSN nicht verwenden oder der Cloud-Modus deaktiviert ist, verwendet Kaspersky Endpoint Security die Vollversion der Programmdatenbanken.

Der Cloud-Modus wird automatisch deaktiviert, wenn KSN deaktiviert ist.

Verwendung des Dienstes für den KSN-Proxyserver

Benutzergeräte, die unter Verwaltung des Administrationsservers stehen, können entweder direkt oder über den KSN Proxy-Service des Administrationsservers mit KSN interagieren.

Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, wird die Interaktion mit der KSN-Infrastruktur über den KSN Proxy-Service realisiert. Wird die direkte Interaktion mit KSN nicht unterstützt. Wenn der KSN-Proxyserver nicht verfügbar ist, wird zur Ausführung der Anwendung kein KSN verwendet.

Der Proxyserver von KSN bietet die folgenden Funktionen:

- Benutzergeräte können selbst dann Anfragen und Informationen an KSN senden, wenn sie über keinen direkten Internetzugriff verfügen.
- Die verarbeiteten Daten werden vom Proxyserver von KSN im Cache zwischengespeichert, wodurch die Belastung für den ausgehenden Datenverkehr verringert und das Empfangen der abgefragten Informationen durch das Benutzergerät beschleunigt wird.

Sie können die Einstellungen des Proxy-Server-Dienstes von KSN in den Eigenschaften des Administrationsservers konfigurieren. Weitere Informationen zum Proxyserver von KSN finden Sie in der Hilfe von Kaspersky Security Center.

Wenn Sie Kaspersky Endpoint Security im Standardmodus verwenden, können Sie mithilfe der Web Console oder der Verwaltungskonsole die Einstellungen zur Verwendung des KSN-Proxyservers für die Anwendungsausführung konfigurieren:

Die Konfiguration der Einstellungen des KSN-Proxyservers über die Befehlszeile ist nicht möglich.

In Kaspersky Security Center können Sie für die Verwendung des KSN-Proxyservers durch Kaspersky Endpoint Security die folgenden Parameter konfigurieren:

- Die Verwendung des Administrationsservers als KSN-Proxyserver aktivieren oder deaktivieren.
- Die direkte Interaktion mit den KSN-Servern erlauben oder verbieten, wenn der KSN Proxy-Service nicht verfügbar ist.

Verwendung von Kaspersky Security Network in der Web Console konfigurieren

In der Web Console können Sie die Verwendung von Kaspersky Security Network durch das Programm in den Richtlinieneigenschaften konfigurieren (**Programmeinstellungen → Allgemeine Einstellungen → Kaspersky Security Network**).

Informationen zur Verfügbarkeit von KSN werden in Kaspersky Security Center anhand des Status des Client-Geräts (*OK, Kritisch, Warnung*) in der Liste der verwalteten Geräte auf der Registerkarte **Assets (Geräte)** angezeigt.

Verwendung von Kaspersky Security Network in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Verwendung von Kaspersky Security Network durch Kaspersky Endpoint Security in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) konfigurieren (**Erweiterter Schutz → Kaspersky Security Network**).

Den Text der Erklärung zu Kaspersky Security Network können Sie im Fenster **Erklärung zu Kaspersky Security Network** lesen, welches Sie über den Link **Erklärung zu Kaspersky Security Network** öffnen können.

Informationen zur Verfügbarkeit von KSN werden in Kaspersky Security Center anhand des Status des Client-Geräts (*OK, Kritisch, Warnung*) in der Liste der verwalteten Geräte auf der Registerkarte **Geräte** angezeigt.

Einstellungen für Kaspersky Security Network

Parameter	Description
Erklärung zu Kaspersky Security Network	Dieser Link öffnet das Fenster **Erklärung zu Kaspersky Security Network**. In diesem Fenster können Sie den Text der Erklärung zu Kaspersky Security Network einsehen.
Kaspersky Security Network (KSN)	In diesem Block werden Informationen darüber angezeigt, welche Option der KSN-Nutzung aktiviert ist und ob KSN zur Ausführung von Kaspersky Endpoint Security verwendet wird oder nicht. Durch Klicken auf die Schaltfläche **Ändern** öffnet sich ein Fenster, in dem Sie die Verwendung des Kaspersky Security Network konfigurieren können.
Cloud-Modus aktivieren	Das Kontrollkästchen aktiviert oder deaktiviert den Ausführungsmodus, in dem Kaspersky Endpoint Security eine schlankere Version der Malware-Datenbanken verwendet. Das Kontrollkästchen ist verfügbar, wenn KSN aktiviert ist. Das Kontrollkästchen ist aktiviert, wenn Sie beim Erstellen der Richtlinie die Bedingungen der Erklärung zu Kaspersky Security Network akzeptiert haben und den erweiterten KSN-Modus verwenden. Der Modus wird nach dem nächsten Update der 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 zum Schutz virtueller Umgebungen kann die Anwendung nur über den KSN-Proxyserver mit der KSN-Infrastruktur interagieren.
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.

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.

Verwendung von Kaspersky Security Network über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Verwendung von Kaspersky Security Network mithilfe des Parameters `UseKSN` in den allgemeinen Anwendungseinstellungen aktivieren und deaktivieren.

Sie können den Wert des Parameters `UseKSN` mithilfe von Befehlszeilenschaltern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen 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>` – Modus zur Verwendung von Kaspersky Security Network.
- `--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 <Pfad zur Konfigurationsdatei> [--json] [--
accept-ksn]
```

wobei:

- `--file <Pfad zur Konfigurationsdatei>` ist der vollständige Pfad zur Konfigurationsdatei mit den allgemeinen Programmeinstellungen, in der der erforderliche `UseKSN`-Wert konfiguriert ist.
- Geben Sie die Option `--json` an, wenn Sie Einstellungen aus einer JSON-Konfigurationsdatei 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 über die Befehlszeile prüfen

Um die Verbindung mit Kaspersky Security Network zu überprüfen, führen Sie den folgenden Befehl aus:

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

Die Zeile **Verwendung von Kaspersky Security Network** zeigt den Status der Verbindung mit Kaspersky Security Network an:

- Wenn als Status `Erweiterter KSN-Modus` angezeigt wird, ist Kaspersky Endpoint Security mit Kaspersky Security Network verbunden: Es können Informationen aus der Wissensdatenbank abgerufen werden und anonyme Statistikdaten und Informationen über die Typen und Quellen der Bedrohungen gesendet werden.
- Wenn als Status `Standardmäßiger KSN-Modus` angezeigt wird, ist Kaspersky Endpoint Security mit Kaspersky Security Network verbunden: Es können Informationen aus der Wissensdatenbank abgerufen werden, aber es werden keine anonymen Statistikdaten und Informationen über die Typen und Quellen der Bedrohungen gesendet.
- Wenn der Status `Nicht aktiviert` angezeigt wird, ist Kaspersky Endpoint Security nicht mit Kaspersky Security Network verbunden.

In der Zeile **Infrastrukturlösung von Kaspersky Security Network**, werden die Informationen zu der Infrastrukturlösung angezeigt, die für die Interaktion mit den Reputationsdatenbanken von Kaspersky verwendet wird: `Kaspersky Security Network` oder `Kaspersky Private Security Network`.

Mögliche Gründe, warum keine Verbindung mit Kaspersky Security Network besteht:

- Das Gerät des Benutzers ist nicht mit dem Internet verbunden.
- Die Verwendung von Kaspersky Security Network ist nicht aktiviert.

- Die 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.

Cloud-Modus über die Befehlszeile aktivieren oder deaktivieren

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 Anwendung 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 den Wert der Einstellung `CloudMode` mithilfe der Konfigurationsdatei, die alle allgemeinen Programmeinstellungen enthält, oder mithilfe von Befehlszeilenschaltern ändern.

> Der Cloud-Modus der Anwendung ist bei aktivierter Verwendung von Kaspersky Security Network verfügbar.

Erweiterte Einstellungen für die Ausführung der Anwendung

Sie können die folgenden zusätzlichen Einstellungen für die Ausführung der Anwendung konfigurieren:

- Proxyserver für die Anwendung.
- Globale Ausschlüsse zum Ausschließen von Mountpunkten aus dem Modul zum Abfangen für Dateioperationen der Komponenten zum Schutz vor bedrohlichen Dateien, zum Schutz vor Verschlüsselung und zur Container-Überwachung, sowie der Aufgaben zur Schadsoftware-Untersuchung, zur Untersuchung wichtiger Bereiche, zur Untersuchung von Containern und zur Untersuchung von Wechseldatenträgern.
- Prozess-Speicher von der Untersuchung ausschließen.
- Modus des Modul zum Abfangen von Dateioperationen.
- Erkennung legaler Programme, die von Angreifern zur Beschädigung von Geräten oder Daten ausgenutzt werden können.
- Überwachung der Anwendungsstabilität.
- Starteinstellungen der Anwendung.
- Begrenzung der Nutzung von Speicher- und CPU-Ressourcen für Untersuchungsaufgaben.
- Begrenzung des von der Anwendung verwendeten residenten Speichers.
- Begrenzung der Anzahl benutzerdefinierter Untersuchungsaufgaben, die ein nicht privilegierter Benutzer gleichzeitig ausführen kann.
- Einstellungen zur Übertragung von Informationen an den Kaspersky Security Center.
- Berechtigungen für die Verwaltung von Aufgaben.
- Geplanter Aufgaben auf einem Gerät abbrechen, das im Akkubetrieb läuft.
- Einstellungen für das Abfangen von Systemereignissen.
- Erweiterte Parameter der Telemetriedaten.

Proxyserver konfigurieren

Sie können die Proxy-Server-Einstellungen konfigurieren, wenn Benutzer von Client-Geräten über einen Proxy-Server auf das Internet zugreifen. Kaspersky Endpoint Security kann einen 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. Sie können die Verwendung des Administrationsservers als Proxyserver für den Zugriff auf Aktivierungsserver in der Web Console und in der Verwaltungskonsole aktivieren.

Sie können die folgenden Ausnahmen bei der Verwendung eines Proxyservers in der Web Console, in der Verwaltungskonsole und in der Befehlszeile konfigurieren:

- Für die Komponenten EDR Expert (on-premise), NDR (KATA) und Sandbox, welche die Integration mit Detection and Response-Lösungen gewährleisten. Sie können die Komponenten angeben, die keinen Proxyserver verwenden sollen.
- Für Webadressen. Sie können eine Liste von Adressen angeben, für deren Verbindung kein Proxyserver verwendet wird.

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. Die Verwendung des Kaspersky Security Center Administrationsservers als Proxyserver für den Zugriff auf die Aktivierungsserver von Kaspersky wird ebenfalls nicht unterstützt.

Proxyserver-Einstellungen in der Web Console konfigurieren

In der Web Console können Sie die Proxyserver-Einstellungen in den Richtlinieneigenschaften (**Programmeinstellungen** → **Allgemeine Einstellungen** → **Netzwerkeinstellungen**) konfigurieren.

Proxyserver-Einstellungen in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Proxy-Einstellungen in den Richtlinieneigenschaften verwalten (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**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.

Parameter	Description
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 die Anwendung im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, stellt der Schutzserver die Lizenzinformationen 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 Anwendungskomponenten, für die kein Proxyserver erforderlich ist: • **Endpoint Detection and Response Expert (on-premise)** – Keinen Proxyserver für die Verbindung mit Servern verwenden, welche die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA) gewährleisten. • **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.

Parameter	Description
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). Sie können die Webadressen in der Tabelle **hinzufügen**, **bearbeiten** und **löschen**. 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.

Proxyserver-Einstellungen über die Befehlszeile konfigurieren

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 den Wert von Parametern mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen enthält.

Der Parameter `UseProxy` kann folgende Werte annehmen:

- `Ja`: Nutzung eines Proxy-Servers aktivieren.
- `No` – Nutzung eines Proxyservers deaktivieren.

Mit der Einstellung `ProxyServer` können Sie Proxyserver-Einstellungen in folgendem Format angeben: `<Verbindungsprotokoll>://[<Benutzer>[:<Kennwort>]@]<Adresse des Proxyservers><code class="programcharacter">a>:<</code>Portnummer>`, wobei gilt:

- `<Benutzer>` ist ein Benutzername für die Authentifizierung am Proxyserver.
- `<Kennwort>` ist ein Benutzerkennwort für die Authentifizierung am Proxyserver.
- `<Proxyserver-Adresse>` – IP-Adresse oder Domänenname des Proxyservers.
- `<Portnummer>` 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 `<Adresse>[:<Portnummer>]` angegeben. Zur Angabe von Adressen können Sie Platzhalter (`*`-Symbole) und Kommentare (nach einem "\"-Symbol) verwenden.

Die folgenden Parameter erlauben die Konfiguration eines Proxyservers bei der Ausführung der 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:

- `Ja`: Nutzung eines Proxy-Servers aktivieren.
- `No` – Nutzung eines Proxyservers deaktivieren.

Globale Ausschlüsse konfigurieren

Sie können globale Ausschlüsse konfigurieren, um Mountpunkte aus dem Modul zum Abfangen für Dateioperationen der folgenden Komponenten und Untersuchungsaufgaben auszuschließen: Komponenten zum Schutz vor bedrohlichen Dateien und zum Schutz vor Verschlüsselung, sowie Aufgaben zur Schadsoftware-Untersuchung, zur Untersuchung wichtiger Bereiche und zur Untersuchung von Containern. Durch das Ausschließen von Mountpunkten können Sie lokale oder Remote-Verzeichnisse, die auf dem Gerät gemountet sind, vom Modul zum Abfangen von Dateioperationen ausschließen. Darüber hinaus wirken sich globale Ausnahmen auf die Ausführung der Komponente zur Container-Überwachung (Untersuchung von Containern, Container-Überwachung) und der Aufgabe Untersuchung von Wechseldatenträgern aus.

Globale Ausschlüsse in der Web Console konfigurieren

In der Web Console können Sie globale Ausnahmen konfigurieren in den Richtlinieneigenschaften (**Programmeinstellungen** → **Vertrauenswürdige Zone** → **Vertrauenswürdige Mount-Points**).

Globale Ausschlüsse in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie globale Ausnahmen in den Richtlinieneigenschaften verwalten (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**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 Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden. 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.

Globale Ausnahmen über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie den Ausschluss von Mountpunkten mithilfe des Parameters `ExcludedMountPoint.item_#` in den allgemeinen Anwendungseinstellungen konfigurieren.

Sie können den Wert des Parameters mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen 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:<Typ des Dateisystems>` – alle eingebundenen Verzeichnisse mit dem angegebenen Dateisystem werden vom Modul zum Abfangen von Dateioperationen ausgeschlossen.
- `/mnt` — Objekte im Mountpunkt /mnt (einschließlich Unterverzeichnissen) vom Abfangen von Dateioperationen ausschließen. Dieses Verzeichnis wird als temporärer Mountpunkt für Wechseldatenträger verwendet.
- `<Pfad, der die Maske /mnt/user* oder /mnt/**/user_share>` enthält — Objekte in Mountpunkten, deren Namen die angegebene **Maske** enthalten, vom Abfangen von Dateioperationen ausschließen.

  Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

  Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

  Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

  Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

  Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben.

  Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst.

  Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

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.

Ausschließen des Prozessspeichers von Untersuchungen

Sie können Untersuchungsausnahmen für den Prozess-Speicher konfigurieren. Der Arbeitsspeicher der angegebenen Prozesse wird von der Anwendung nicht untersucht.

Ausschlüsse in der Web Console konfigurieren

In der Web Console können Sie in den Richtlinieneigenschaften das Ausschließen des Prozessspeichers von Untersuchungen konfigurieren (**Programmeinstellungen** → **Allgemeine Einstellungen** → **Leistung**).

Ausschlüsse in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie Ausnahmen für den Prozessspeicher in den Richtlinieneigenschaften verwalten (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Allgemeine Einstellungen** → **Prozessspeicher ausschließen**).

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 Sie **Masken** verwenden. Standardmäßig ist die Liste leer.

Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben.

Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst.

Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Sie können 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.

Ausschlüsse über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie Untersuchungsausschlüsse für den Prozess-Speicher mithilfe des Parameters `MemScanExcludedProgramPath.item_#` in den allgemeinen Anwendungseinstellungen konfigurieren.

Sie können den Wert des Parameters mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen enthält.

Der Parameter `MemScanExcludedProgramPath.item_#` enthält den vollständigen Pfad zum Prozess im lokalen Verzeichnis. Bei der Angabe des Pfades können Sie **Masken** verwenden.

Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Sie können mehrere Prozesse angeben, die von der Untersuchung ausgeschlossen werden sollen.

Modus des Interceptors von Dateioperationen auswählen

Der Modus des Interceptors von Dateioperationen hat Auswirkungen auf die Ausführung der Komponenten Schutz vor bedrohlichen Dateien und Gerätekontrolle.

- Die Anwendung kann den Zugriff auf Dateien blockieren, die während der Untersuchung der Komponente "Schutz vor bedrohlichen Dateien" geprüft werden. Der Zugriff ist standardmäßig blockiert: Jeder Zugriff auf eine zu untersuchende Datei wartet auf das Resultat der Untersuchung. Wenn die Untersuchung in der Datei keine Bedrohungen erkennt, erlaubt die Anwendung den Zugriff auf die Datei. Wenn infizierte Objekte gefunden werden, führt die Anwendung die im Parameter **Aktionen beim Erkennen von Bedrohungen** (`ActionOnThreat`) der Komponente "Schutz vor bedrohlichen Dateien" angegebenen Aktionen aus.

  Sie können das Blockieren des Zugriffs auf Dateien, die von der Komponente "Schutz vor bedrohlichen Dateien" untersucht werden, deaktivieren. In diesem Fall erfolgt die Untersuchung asynchron.

- Die Anwendung kann den Zugriff auf Dateien auf einem Gerät blockieren, während Gerätekontrolle bestimmt, ob der Zugriff auf das Gerät gewährt werden kann. Der Zugriff ist standardmäßig blockiert: Jeder Dateizugriff auf dem kontrollierten Gerät wartet auf das Resultat der Untersuchung. Die Anwendung gewährt den Zugriff auf Dateien, wenn aufgrund des Untersuchungsergebnisses der Gerätekontrolle der Zugriff auf das Gerät mit den Dateien erlaubt ist.

  Sie können das Blockieren des Zugriffs auf Dateien auf einem Gerät, das von der Komponente "Gerätekontrolle" kontrolliert wird, deaktivieren. In diesem Fall bestimmt die Gerätekontrolle, ob ein Zugriff auf das Gerät möglich ist, asynchron.

Wenn sich der Interceptor für Dateioperationen nicht im Blockiermodus befindet, werden die Komponenten Schutz vor bedrohlichen Dateien, Gerätekontrolle und Ausführungsprävention von Objekten unabhängig vom festgelegten Modus im Benachrichtigungs-Modus ausgeführt.

Konfiguration in der Web Console

In der Web Console können Sie in den Richtlinieneigenschaften (**Programmeinstellungen** → **Allgemeine Einstellungen** → **Erkennungseinstellungen**) den Modus zum Abfangen von Dateivorgängen konfigurieren.

Konfiguration in der Verwaltungskonsole

In der Verwaltungskonsole können Sie in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Richtlinie mithilfe der Verwaltungskonsole erstellen) (**Allgemeine Einstellungen** → **Programmeinstellungen** → Abschnitt **Modus zum Abfangen von Dateivorgängen**) die Einstellungen der Programmablaufverfolgung verwalten.

Das Kontrollkästchen **Zugriff auf Dateien während der Untersuchung blockieren** aktiviert oder deaktiviert den Zugriff auf Dateien während der Untersuchung durch die Komponenten "Schutz vor bedrohlichen Dateien" und "Gerätekontrolle".

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.

Konfiguration 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.

Sie können den Wert des Parameters mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen enthält.

Der Parameter `FileBlockDuringScan` kann folgende Werte annehmen:

- `Yes` (Standardwert) – blockiert den Zugriff auf Dateien während der Untersuchung durch die Komponenten "Schutz vor bedrohlichen Dateien" und "Gerätekontrolle".
- `No` – Zugriff auf Dateien während des Untersuchung nicht blockieren. Der Zugriff auf eine beliebige Datei ist erlaubt, die Überprüfung erfolgt im asynchronen Modus.

  Dieser Modus des Interceptors von Dateioperationen hat während der Ausführung weniger Auswirkungen auf die Systemleistung. Es besteht jedoch das Risiko, dass eine Bedrohung in einer Datei nicht desinfiziert oder entfernt wird, wenn diese Datei beispielsweise während der Untersuchung ihren Namen ändert, bevor die Anwendung eine Entscheidung über den Status dieser Datei treffen kann.

Erkennen von Anwendungen konfigurieren, die von Angreifern für Kompromittierungen ausgenutzt werden können

Aktivieren und deaktivieren Sie die Erkennung von legitimen Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können. Diese Anwendungen selbst enthalten keine schädlichen Funktionen, können aber von Angreifern ausgenutzt werden. Ausführliche Informationen über legitime Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Benutzerdaten ausgenutzt werden können, finden Sie auf der Website der Kaspersky Encyclopedia.

Konfiguration in der Web Console

In der Web Console können Sie die Erkennungseinstellungen für legitime Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können, in den Richtlinieneigenschaften verwalten (**Programmeinstellungen** → **Allgemeine Einstellungen** → **Erkennungseinstellungen**).

Konfiguration in der Verwaltungskonsole

In der Verwaltungskonsole können Sie die Erkennung legitimer Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können, in den Richtlinieneigenschaften aktivieren und deaktivieren (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Allgemeine Einstellungen** → **Programmeinstellungen**, Abschnitt **Untersuchungseinstellungen**).

Das Kontrollkästchen **Legale Programme erkennen, die von Angreifern zur Beschädigung von Geräten oder Daten ausgenutzt werden können** aktiviert oder deaktiviert das Erkennen legaler Programme, die von Angreifern zur Beschädigung von Geräten oder Daten ausgenutzt werden können.

Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Konfiguration über die Befehlszeile

Über die Befehlszeile können Sie die Erkennung legitimer Anwendungen, die von Angreifern für Kompromittierungen von Geräten oder Daten ausgenutzt werden können, mithilfe des Parameters `DetectOtherObjects` in den allgemeinen Programmeinstellungen aktivieren und deaktivieren.

Sie können den Wert des Parameters mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen enthält.

Der Parameter `DetectOtherObjects` kann folgende Werte annehmen:

- `Yes` – Aktiviert die Erkennung legaler Programme, die von Angreifern zur Beschädigung von Geräten oder Daten ausgenutzt werden können.
- `No` – Deaktiviert die Erkennung legaler Programme, die von Angreifern zur Beschädigung von Geräten oder Daten ausgenutzt werden können.

Überwachung der Anwendungsstabilität aktivieren

Sie können der Überwachung der Anwendungsstabilität von Kaspersky Endpoint Security aktivieren oder deaktivieren, mit der Sie die Anzahl der ungeplanten Unterbrechungen der Anwendung verfolgen und den Administrator über den instabilen Betrieb der Anwendung informieren können. Darüber hinaus können Sie die Überwachungseinstellungen konfigurieren.

Konfiguration in der Web Console

In der Web Console können Sie die Überwachung der Programmstabilität in den Richtlinieneigenschaften aktivieren oder deaktivieren (**App-Einstellungen** → Allgemeine Einstellungen → **Leistung**).

Konfiguration in der Verwaltungskonsole

In der Verwaltungskonsole können Sie die Überwachung der Programmstabilität in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) aktivieren oder deaktivieren (**Allgemeine Einstellungen** → **Programmeinstellungen**, **Erweiterte Programmeinstellungen**).

Das Kontrollkästchen **Überwachung der Anwendungsstabilität aktivieren** aktiviert oder deaktiviert die Überwachung der Anwendungsstabilität von Kaspersky Endpoint Security.

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>*.

Konfiguration 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.

Starteinstellungen der Anwendung konfigurieren

Sie können die Starteinstellungen der Anwendung konfigurieren.

Begrenzung in der Web Console konfigurieren

In der Web Console können Sie die Einstellungen für den Programmstart in den Richtlinieneigenschaften verwalten (**App-Einstellungen** → **Allgemeine Einstellungen** → **Interaktion mit dem Benutzer**).

Begrenzung in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen für den Programmstart in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) verwalten (**Allgemeine Einstellungen** → **Programmeinstellungen**, **Einstellungen für den Programmstart**).

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.

Begrenzung über die Befehlszeile konfigurieren

In der Befehlszeile können Sie Starteinstellungen der Anwendung 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 Werte von 1 bis 10 annehmen. Standardwert: 5.

Mit dem Parameter `StartupTimeout` können Sie die maximale Wartezeit (in Minuten) auf den Start der Anwendung festlegen, nach deren Überschreitung der Prozess "kesl" neu gestartet wird. Der Parameter kann die Werte 1 bis 60 annehmen. Standardwert: 3.

Begrenzung des von der Anwendung verwendeten residenten Speichers

Sie können die Nutzung des residenten Speichers für das Programm begrenzen. Standardmäßig wird die Begrenzung automatisch festgelegt.

Begrenzung in der Web Console konfigurieren

In der Web Console können Sie die Beschränkung für die Nutzung des residenten Speichers in den Richtlinieneigenschaften verwalten (**App-Einstellungen** → **Allgemeine Einstellungen** → **Leistung**).

Begrenzung in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) eine Beschränkung für die Nutzung des residenten Speichers festlegen (**Allgemeine Einstellungen** → **Programmeinstellungen**).

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

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.

Begrenzung über die Befehlszeile konfigurieren

In der Befehlszeile können Sie die Beschränkung für die Nutzung des residenten Speichers mithilfe der Einstellung `MaxMemory` in der Konfigurationsdatei kesl.ini konfigurieren.

Der Parameter `MaxMemory` kann folgende Werte annehmen:

- `off` – Die Nutzung des residenten Speichers ist nicht beschränkt.
- `<Wert>%` – ein Wert zwischen 1 und 100 Prozent des Arbeitsspeichers.
- `<Wert>MB` – ein Wert in Megabyte.
- `lowest/<Wert>%/<Wert>MB` – der kleinere Wert aus Prozentwert und absolutem Wert in Megabyte.

- `highest/<Wert>%/<Wert>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`.

Begrenzung der verwendeten Speicher- und CPU-Ressourcen

Sie können die Speichernutzung durch Untersuchungsaufgaben begrenzen. Das Standardlimit beträgt 8192 MB.

> Es wird empfohlen, das Speichernutzungslimit für Untersuchungsvorgänge niedriger anzusetzen als das Limit für die residente Speichernutzung, um zu vermeiden, dass Untersuchungsvorgänge den gesamten verfügbaren Speicher belegen und die Anwendung neu starten.

Sie können eine Begrenzung der Nutzung von CPU-Ressourcen für Untersuchungsaufgaben konfigurieren. Standardmäßig ist keine Begrenzung festgelegt. Beim Einrichten der Obergrenze sollte beachtet werden, dass 100% für die aufsummierten Ressourcen aller Prozessorkerne steht. 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 vom Dienstprogramm `top` gemeldete Wert auf derselben 10-Kern-CPU unter 150 % gehalten wird, müssen Sie `15` als Begrenzung der CPU-Auslastung angeben. Die Begrenzung der CPU-Auslastung muss eine ganze Zahl von 10 bis 100 sein. Darüber hinaus wird die Obergrenze für die Prozessornutzung nicht auf alle, sondern nur auf die folgenden Aufgaben der Anwendung angewendet: *Schadsoftware-Untersuchung*, *Untersuchung wichtiger Bereiche*, *Inventarisierung* und *Untersuchung von Containern*. Daher kann die CPU-Auslastung auch bei aktiver Begrenzung höher ausfallen als beabsichtigt.

Begrenzung in der Web Console konfigurieren

In der Web Console können Sie die Einstellungen zur Begrenzung der CPU- und Speichernutzung für Untersuchungsaufgaben in den Richtlinieneigenschaften verwalten (**Programmeinstellungen** → **Allgemeine Einstellungen** → **Leistung**).

Begrenzung in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) die Begrenzung der CPU-Auslastung aktivieren oder deaktivieren und eine Begrenzung des Arbeitsspeichers für Untersuchungsaufgaben konfigurieren (**Allgemeine Einstellungen** → **Programmeinstellungen**, Abschnitt **Leistung**).

Durch Klick auf die Schaltfläche **Konfigurieren** im Block **Leistung** wird das Fenster **Leistungseinstellungen für Untersuchungsaufgaben** geöffnet. Dort können Sie im Block **Prozessor- und Speicherauslastung** Einschränkungen anpassen (siehe Tabelle unten).

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 die maximale Auslastung aller CPU-Kerne für diese Aufgaben unter dem im Feld rechts angegebenen Prozentwert gehalten (die maximale Gesamtauslastung aller CPU-Kerne wird als 100 % angesetzt). 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.

Begrenzung über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie Grenzwerte für die CPU-Auslastung für die Aufgaben *ODS*, *ContainerScan* und *InventoryScan* mithilfe der Einstellungen `UseOnDemandCPULimit` und `OnDemandCPULimit` in den allgemeinen Programmeinstellungen konfigurieren.

Sie können den Wert von Parametern mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen enthält.

Der Parameter `UseOnDemandCPULimit` kann folgende Werte annehmen:

- `Yes` – Aktiviert die Begrenzung der Nutzung von CPU-Ressourcen für die Aufgabentypen *ODS*, *ContainerScan* und *InventoryScan*.
- `No` – Deaktiviert die Begrenzung der Nutzung von CPU-Ressourcen für Aufgaben.

Mit dem Parameter `OnDemandCPULimit` können Sie die maximale Auslastung aller Prozessorkerne (in Prozent) bei der Ausführung der Aufgabentypen *ODS*, *ContainerScan* und *InventoryScan* angeben. Der Wert des Parameters muss eine Ganzzahl zwischen 10 und 100 sein. Standardwert: 100.

Über die Befehlszeile können Sie Grenzwerte für die Speichernutzung für die Aufgaben *ODS*, *ContainerScan* und *InventoryScan* mithilfe der Einstellung `ScanMemoryLimit` in der Konfigurationsdatei kesl.ini konfigurieren. Standardwert: 8192.

Begrenzung der Anzahl der Aufgaben zur benutzerdefinierten Untersuchung

Sie können die Anzahl der Aufgaben zur benutzerdefinierten Untersuchung, die ein nicht privilegierter Benutzer gleichzeitig auf einem Gerät ausführen kann, begrenzen. Es gibt keine Begrenzung für die Anzahl der Aufgaben, die ein Root-Benutzer ausführen kann.

Begrenzung in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Richtlinie mithilfe der Verwaltungskonsole erstellen) (**Allgemeine Einstellungen** → **Programmeinstellungen**, Abschnitt **Leistung**) den Grenzwert für die Anzahl gleichzeitig ausgeführter Aufgaben zur benutzerdefinierten Untersuchung konfigurieren, die ein nicht privilegierter Benutzer auf dem Gerät ausführen kann.

Durch Klick auf die Schaltfläche **Konfigurieren** im Block **Leistung** wird das Fenster **Leistungseinstellungen für Untersuchungsaufgaben** geöffnet. Dort können Sie im Block **Anzahl der benutzerdefinierten Untersuchungsaufgaben** im Eingabefeld **Maximale Anzahl benutzerdefinierter Untersuchungsaufgaben** einen Wert zwischen 0 und 100.000 angeben. Standardwert: 0. Wenn der Wert 0 angegeben ist, kann ein nicht privilegierter Benutzer keine Aufgaben zur benutzerdefinierten Untersuchung starten.

Begrenzung über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie mithilfe des Parameters `LimitNumberOfScanFileTasks` in den allgemeinen Anwendungseinstellungen die Anzahl der gleichzeitig ausgeführten benutzerdefinierten Untersuchungsaufgaben begrenzen.

Sie können den Wert des Parameters mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen enthält.

Der Parameter `LimitNumberOfScanFileTasks` kann Werte von 0 bis 100000 annehmen. Wenn der Wert 0 angegeben ist, kann ein nicht privilegierter Benutzer keine Aufgaben zur benutzerdefinierten Untersuchung starten. Standardwert: 5.

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.

Eine Liste der von Kaspersky-Lab-Anwendungen auf Client-Geräten unter Quarantäne gestellten Dateien wird in Kaspersky Security Center erstellt und ist in der Web Console (**Vorgänge** → **Speicher** → **Quarantäne**) und in der Verwaltungskonsole (**Erweitert** → **Speicher** → **Quarantäne**) verfügbar.

Eine Liste der Dateien, die von Kaspersky-Lab-Anwendungen auf Client-Geräten im Backup abgelegt wurden, wird in Kaspersky Security Center erstellt und ist in der Web Console (**Vorgänge** → **Speicher** → **Backup**) und in der Verwaltungskonsole (**Erweitert** → **Speicher** → **Backup**) verfügbar.

Informationen zu nicht verarbeiteten Dateien werden in der Liste der aktiven Bedrohungen in Web Console (**Vorgänge** → **Speicher** → **Aktive Bedrohungen**) und in der Verwaltungskonsole (**Erweitert** → **Speicher** → **Aktive Bedrohungen**) angezeigt.

Informationen zu Geräten, die auf einem Client-Gerät installiert oder mit diesem verbunden sind, werden in der Liste der Geräte in der Web Console (**Vorgänge** → **Speicher** → **Geräte**) und in der Verwaltungskonsole (**Erweitert** → **Speicher** → **Geräte**) angezeigt. Informationen werden übertragen, wenn die Komponente Gerätekontrolle aktiviert ist.

Informationen zu Anwendungen, die auf einem Client-Gerät gefunden wurden, werden als Liste in der Web Console (**Vorgänge** → **Drittanbieter-Anwendungen** → **Anwendungsregister**) oder der Verwaltungskonsole (**Erweitert** → **Anwendungsverwaltung** → **Anwendungsregister**) angezeigt. Die Informationen werden übertragen, wenn die Komponente Programmkontrolle aktiviert ist.

Übertragung von Informationen in der Web Console aktivieren und deaktivieren

In der Web Console können Sie die Einstellungen für die Integration mit dem Administrationsserver in den Richtlinieneigenschaften (**Programmeinstellungen** → **Allgemeine Einstellungen** → **KSC-Integration**, Abschnitt **Datenübertragung an den Administrationsserver**, Link **Erweiterte Einstellungen**) und in den Eigenschaften des verwalteten Geräts (**Assets (Geräte)** → **Verwaltete Geräte** → Link <device name> → Registerkarte **Programme** → Link <Kaspersky Endpoint Security application name> → Registerkarte **Programmeinstellungen** → Abschnitt **Speichereinstellungen**, Abschnitt **Einstellungen für die Datenübertragung an den Administrationsserver**) verwalten.

Die Parameter für die Datenübertragung an den Administrationsserver in den Richtlinieneigenschaften der Web Console werden in Anhang 5 beschrieben.

Die Parameter für die Datenübertragung an den Administrationsserver in den Eigenschaften des verwalteten Geräts werden in der folgenden Tabelle beschrieben.

Parameter für die Datenübertragung an den Administrationsserver in den Geräteeigenschaften

Parameter	Description
Über Dateien des Backup-Speichers informieren.	Das Kontrollkästchen aktiviert oder deaktiviert die Übertragung von Informationen über Dateien im Backup an den Administrationsserver. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Über Dateien in der Quarantäne informieren	Das Kontrollkästchen aktiviert oder deaktiviert die Übertragung von Informationen über unter Quarantäne gestellte Dateien an den Administrationsserver. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
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. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Über installierte oder angeschlossene Geräte informieren	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 deaktiviert.
Über Anwendungen, die auf dem Gerät gefunden wurden, 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. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Datenübertragung in der Verwaltungskonsole aktivieren und deaktivieren

In der Verwaltungskonsole können Sie die Datenübertragung an den Administrationsserver in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**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.

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 den Benutzern das Anzeigen und Ändern lokaler Aufgaben verbietet, sind Informationen über die Aufgaben Scan_My_Computer, Critical_Areas_Scan, Container_Scan, Inventory_Scan, Update (im Standardmodus) und Rollback (im Standardmodus) nicht verfügbar.

- Berechtigung zum Anzeigen und Verwalten von Aufgaben auf Client-Geräten, die in Kaspersky Security Center erstellt wurden.

Konfiguration in der Web Console

In der Web Console können Sie die Einstellungen für Berechtigungen zum Anzeigen und Verwalten von Aufgaben in den Richtlinieneigenschaften (**Programmeinstellungen → Allgemeine Einstellungen → Interaktion mit dem Benutzer**) verwalten.

Konfiguration in der Verwaltungskonsole

In der Verwaltungskonsole können Sie Berechtigungen zum Anzeigen und Verwalten von Aufgaben in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Lokale Aufgaben → Aufgabenverwaltung**) verwalten.

Einstellungen der 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.

Ausführung von Aufgaben im Akkubetrieb beenden

Auf Geräten, die im Akkubetrieb laufen, können Sie das Abbrechen von geplanten Aufgabenausführungen aktivieren und deaktivieren. Durch das Abbrechen geplanter Aufgabenausführungen können Sie den Ressourcenverbrauch senken und die Akkulaufzeit verlängern.

Wenn das Gerät bei aktiviertem Abbruch geplanter Aufgaben im Akkubetrieb läuft, bricht Kaspersky Endpoint Security die geplanten Ausführungen für folgende Aufgaben ab:

- alle Untersuchungsaufgaben (benutzerdefinierte Untersuchung, Container-Untersuchung, benutzerdefinierte Container-Untersuchung, Untersuchung wichtiger Bereiche, Schadsoftware-Untersuchung)
- Inventarisierung
- Datenbanken und Module der Anwendung aktualisieren

- IOC-Untersuchung
- Überwachung der System-Integrität

Bei Bedarf können Sie die erforderlichen Aufgaben manuell ausführen.

Konfiguration in der Web Console

In der Web Console können Sie den Abbruch geplanter Aufgaben in den Richtlinieneigenschaften konfigurieren (**Programmeinstellungen** → **Allgemeine Einstellungen** → **Performance**).

Konfiguration in der Verwaltungskonsole

In der Verwaltungskonsole können Sie den Abbruch geplanter Aufgaben in den Richtlinieneigenschaften verwalten (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Allgemeine Einstellungen** → **Programmeinstellungen**, **Leistung**).

Das Kontrollkästchen **Geplante Aufgaben im Akkubetrieb überspringen** aktiviert oder deaktiviert das Überspringen von Aufgaben, die nach Zeitplan ausgeführt werden.

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).

Konfiguration über die Befehlszeile

Über die Befehlszeile können Sie das Abbrechen geplanter Aufgabenausführungen mithilfe des Parameters `PowerSaveMode` in den allgemeinen Einstellungen der Anwendung konfigurieren.

Sie können den Wert des Parameters mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen enthält.

Der Parameter `PowerSaveMode` kann folgende Werte annehmen:

- `Ja` (Standardwert) – Geplante Aufgaben auf einem Gerät, das im Akkubetrieb läuft, überspringen.
- `Nein` – Geplante Aufgaben auf einem Gerät unabhängig von der Stromquelle (Netz oder Akku) planmäßig ausführen.

Abfangen von Systemereignissen konfigurieren

Um ordnungsgemäß zu funktionieren, muss die Anwendung Systemereignisse im Sinne von Dateivorgängen und gestarteten Prozessen abfangen. Wenn das Abfangen von Systemereignissen von der Anwendung nicht verwendet wird, findet keine Dateiuntersuchung in Echtzeit statt. Dies reduziert die Schutzstufe des Geräts.

Wenn das Betriebssystem des Geräts die fanotify-Technologie unterstützt, können Sie auswählen, welchen Mechanismus die Anwendung zum Abfangen von Systemereignissen verwenden soll:

- Abfangmechanismus auf Basis der fanotify-Technologie. Dieser Mechanismus wird standardmäßig verwendet.
- Abfangmechanismus auf Basis des *aktualisierbaren Kernel-Moduls*. Die Verwendung des aktualisierbaren Kernel-Moduls optimiert das Abfangen von Dateivorgängen und Prozessstarts durch Kaspersky Endpoint Security. Das aktualisierbare Kernel-Modul fängt Dateivorgänge beim Öffnen, Umbenennen und Ändern von Dateien ab. 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.

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

Für Betriebssysteme, von denen die fanotify-Technologie nicht unterstützt wird, steht die Auswahl des Abfangmechanismus nicht zur Verfügung. Die Anwendung verwendet ein spezielles Kernel-Modul, um Systemereignisse abzufangen und dadurch den Schutz vor bedrohlichen Dateien zu realisieren. Dieses Modul wird beim Start des Schutzes vor bedrohlichen Dateien automatisch kompiliert, sofern die zur Kompilierung erforderlichen Pakete und Tools vorhanden sind.

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).
- Astra Linux Special Edition RUSB.10015-01 (reguläres Update 1.7).
- Astra Linux Special Edition RUSB.10015-01 (reguläres Update 1.8).

  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 Stream 8
- Debian GNU/Linux 12.0
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 8.10
- SberLinux 8.10
- SberLinux 9.1

- SberLinux 9.6
- SberLinux 9.7
- SberOS 3.4.
- SberOS 3.5.
- Ubuntu 22.04 LTS
- Ubuntu 24.04 LTS
- ALT SP Workstation Release 10
- ALT SP Server Release 10
- ALT Education 10
- ALT Workstation Release 11
- ALT Server Release 11
- ALT Education 11
- RED OS 7.3
- RED OS 8
- ROSA Cobalt 7.9 Workstation
- ROSA Cobalt 7.9 Server
- ROSA Chrome 12 Workstation
- ROSA "Chrom" 12 Server

32-Bit-Betriebssysteme und Betriebssysteme für die Arm-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.

Anhand des Tools "Kaspersky ULKM" können Sie prüfen, ob Ihr Gerät die Voraussetzungen für die Installation des aktualisierbaren Kernel-Moduls erfüllt.

Wenn Ihr Betriebssystem den Anforderungen entspricht, können Sie während der Installation der Anwendung den Abfangmechanismus auf Basis des aktualisierbaren Kernel-Moduls auswählen. Daraufhin wird das aktualisierbare Kernel-Modul installiert. Sie können das aktualisierbare Kernel-Modul auch später installieren, wenn Ihr Betriebssystem die Unterstützung erhält. 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. Sie können den Mechanismus zum Abfangen von Systemereignissen in der **Web Console**, der Verwaltungskonsole und in der **Befehlszeile** auswählen.

   In der Befehlszeile können Sie die Einstellungen zum Abfangen von Systemereignissen anhand der Parameter `InterceptorMode`, `InterceptorFallbackStrategy` und `InterceptorApplyStrategy` in den allgemeinen Anwendungseinstellungen konfigurieren.

   > Diese Parameter werden nur angezeigt und können nur geändert werden, wenn das Betriebssystem des Geräts die fanotify-Technologie unterstützt.

   Sie können den Wert von Parametern mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen enthält.

   Der Parameter `InterceptorMode` wählt den Mechanismus zum Abfangen von Systemereignissen aus, der von der Anwendung verwendet wird. Der Parameter kann die folgenden Werte annehmen:

   - `UseFanotify`, um die fanotify-Technologie zum Abfangen von Systemereignissen zu verwenden.
   - `UseUpdatableKernelModule` – Aktualisierbares Kernel-Modul zum Abfangen von Systemereignissen verwenden.

   Der Parameter `InterceptorFallbackStrategy` wird angewendet, wenn das aktualisierbare Kernel-Modul ausgewählt ist. Der Parameter legt die von der Anwendung ausgeführte Aktion fest, falls das aktualisierbare Kernel-Modul aufgrund eines Fehlers nicht gestartet werden kann. Der Parameter kann die folgenden Werte annehmen:

   - `FallbackToFanotify` – Geht zur Verwendung der fanotify-Technologie zum Abfangen von Systemereignissen über, falls das aktualisierbare Kernel-Modul aufgrund eines Fehlers nicht gestartet werden kann.
   - `FallbackToLimitedMode` – Es werden keine Systemereignisse abgefangen, falls das aktualisierbare Kernel-Modul aufgrund eines Fehlers nicht gestartet werden kann. Wenn das Abfangen von Systemereignissen von der Anwendung nicht verwendet wird, findet keine Dateiuntersuchung in Echtzeit statt. Dies reduziert die Schutzstufe des Geräts.

Der Parameter `InterceptorApplyStrategy` wird angewendet, wenn das aktualisierbare Kernel-Modul ausgewählt ist. 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:

- `RestartServiceAutomatically` (empfohlener Wert) – 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.

In der Web Console können Sie das Abfangen von Systemereignissen in den Richtlinieneigenschaften (**Programmeinstellungen** → **Allgemeine Einstellungen** → **Einstellungen für die Interaktion mit dem Betriebssystem**) konfigurieren.

Die Parameter werden nur auf Geräten angewendet, deren Betriebssystem die fanotify-Technologie unterstützt.

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.

Damit die Anwendung ordnungsgemäß funktioniert, muss der Übergang zur Verwendung des aktualisierbaren Kernel-Moduls nach dem automatischen Neustart der Anwendung erfolgen.

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.

Sie können Informationen zum Status und zur Verfügbarkeit des aktualisierbaren Kernel-Moduls auf einem Gerät anzeigen:

- In der Web Console oder in der Verwaltungskonsole mithilfe des Status der Funktionskomponente **Aktualisierbares Kernel-Modul**.
- Über die Befehlszeile anhand der Ausgabe des Befehls `kesl-control --app-info`.

Informationen zum Zustand des aktualisierbaren Kernel-Moduls werden als Statuswerte angezeigt:

- **Gestartet** – das Modul ist installiert und wird ausgeführt.
- **Angehalten** – das Modul ist installiert, wird aber nicht ausgeführt.

- **Nicht verfügbar** – das Modul wird auf dem Gerät nicht unterstützt.
- **Ausführungsfehler** – beim Starten des Moduls ist ein Fehler aufgetreten und das Modul wird nicht ausgeführt.

Möglichkeit zur Installation des aktualisierbaren Kernel-Moduls überprüfen

Anhand des Tools "Kaspersky ULKM" können Sie prüfen, ob Ihr Gerät die Voraussetzungen für die Installation des aktualisierbaren Kernel-Moduls erfüllt.

So starten Sie das Tool mithilfe der Kaspersky Security Center 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.

   So installieren Sie den Administrationsagenten

   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.

4. Erstellen und starten Sie in der Kaspersky Security Center Web Console bzw. in der Verwaltungskonsole eine Aufgabe zur Remote-Installation der Anwendungen für jene Geräte, für die Sie prüfen möchten, ob Sie die Anforderungen erfüllen. Wählen Sie in den Parametern der Aufgabe das von Ihnen erstellte Installationspaket aus.

   Eine Beschreibung des Verfahrens zur Remote-Installation finden Sie in der Hilfe zu Kaspersky Security Center.

   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.
- *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.

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.

"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 nach der Behebung des Ausführungsproblems das aktualisierbare Kernel-Modul wiederzuverwenden, müssen Sie den "abgesicherten" Modus deaktivieren.

So deaktivieren Sie den "abgesicherten" Ausführungsmodus der Anwendung:

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
   ```

Einstellungen für das Abfangen in der Web Console konfigurieren

In der Web Console können Sie das Abfangen von Systemereignissen in den Richtlinieneigenschaften (**Programmeinstellungen → Allgemeine Einstellungen → Einstellungen für die Interaktion mit dem Betriebssystem**) konfigurieren.

Die Parameter werden nur auf Geräten angewendet, deren Betriebssystem die fanotify-Technologie unterstützt.

Einstellungen für das Abfangen in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen für das Abfangen von Systemereignissen in den Eigenschaften der Richtlinie verwalten (Verwalten von Richtlinien in der Verwaltungskonsole, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Allgemeine Einstellungen →Einstellungen für die Interaktion mit dem Betriebssystem**, **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.

Einstellungen für das Abfangen über die Befehlszeile konfigurieren

In der Befehlszeile können Sie die Einstellungen zum Abfangen von Systemereignissen anhand der Parameter `InterceptorMode`, `InterceptorFallbackStrategy` und `InterceptorApplyStrategy` in den allgemeinen Anwendungseinstellungen konfigurieren.

Diese Parameter werden nur angezeigt und können nur geändert werden, wenn das Betriebssystem des Geräts die fanotify-Technologie unterstützt.

Sie können den Wert von Parametern mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen enthält.

Der Parameter `InterceptorMode` wählt den Mechanismus zum Abfangen von Systemereignissen aus, der von der Anwendung verwendet wird. Der Parameter kann die folgenden Werte annehmen:

- `UseFanotify`, um die fanotify-Technologie zum Abfangen von Systemereignissen zu verwenden.
- `UseUpdatableKernelModule` – Aktualisierbares Kernel-Modul zum Abfangen von Systemereignissen verwenden.

Der Parameter `InterceptorFallbackStrategy` wird angewendet, wenn das aktualisierbare Kernel-Modul ausgewählt ist. Der Parameter legt die von der Anwendung ausgeführte Aktion fest, falls das aktualisierbare Kernel-Modul aufgrund eines Fehlers nicht gestartet werden kann. Der Parameter kann die folgenden Werte annehmen:

- `FallbackToFanotify` – Geht zur Verwendung der fanotify-Technologie zum Abfangen von Systemereignissen über, falls das aktualisierbare Kernel-Modul aufgrund eines Fehlers nicht gestartet werden kann.

- `FallbackToLimitedMode` – Es werden keine Systemereignisse abgefangen, falls das aktualisierbare Kernel-Modul aufgrund eines Fehlers nicht gestartet werden kann. Wenn das Abfangen von Systemereignissen von der Anwendung nicht verwendet wird, findet keine Dateiuntersuchung in Echtzeit statt. Dies reduziert die Schutzstufe des Geräts.

Der Parameter `InterceptorApplyStrategy` wird angewendet, wenn das aktualisierbare Kernel-Modul ausgewählt ist. 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:

- `RestartServiceAutomatically` (empfohlener Wert) – 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.

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.

Konfiguration in der Web Console

In der Web Console können Sie erweiterte Einstellungen für Telemetriedaten in den Richtlinieneigenschaften (**Programmeinstellungen → Allgemeine Einstellungen → Einstellungen für die Interaktion mit dem Betriebssystem**) verwalten.

Konfiguration in der Verwaltungskonsole

In der Verwaltungskonsole können Sie zusätzliche Einstellungen für Telemetriedaten in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Allgemeine Einstellungen →Einstellungen für die Interaktion mit dem Betriebssystem**, **Zusätzliche Einstellungen für Telemetriedaten**) verwalten.

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.

Konfiguration über die Befehlszeile

Über die Befehlszeile können Sie zusätzliche Einstellungen für Telemetriedaten mithilfe der Einstellungen `TelemetrySource` und `UseTelemetryMonopolyMode` der vordefinierten Aufgabe Behavior_Detection verwalten.

Sie können die Einstellungen ändern, indem Sie den Befehl `kesl-control --set-settings 20` verwenden, die Konfigurationsdatei bearbeiten, die alle Einstellungen der Aufgabe enthält, oder Befehlszeilenoptionen im Format `< Einstellungsname >=< Einstellungswert >` verwenden.

Der Parameter `TelemetrySource` gibt die Quelle der Telemetriedaten an. Der Parameter kann die folgenden Werte annehmen:

- `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.

Mit dem Parameter `UseTelemetryMonopolyMode` legen Sie den Nutzungsmodus des auditd-Dienstes fest, wenn dieser zur Erfassung von Telemetriedaten verwendet wird. Der Parameter kann die folgenden Werte annehmen:

- `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.

Zum Speichern der Backup-Kopien wird standardmäßig das Verzeichnis "/var/opt/kaspersky/kesl/common/objects-backup/" verwendet. In diesem Verzeichnis werden auch Dateien gespeichert, die in die Quarantäne verschoben wurden. Sie können das Speicherverzeichnis für die Objekte des Backup-Speichers und der Quarantäne über die Befehlszeile ändern.

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.

Sie können die Parameter des Backups auf dem Gerät mittels Richtlinie über die Web Console, die Verwaltungskonsole oder die Befehlszeile konfigurieren. Sie können die folgenden Backup-Einstellungen konfigurieren:

- Speicherzeit von Objekten im Backup. Standardmäßig werden Objekte 30 Tage lang gespeichert.
- Maximale Backup-Größe. Standardmäßig ist die Größe des Backups unbegrenzt.

Pfad zum Verzeichnis, in dem die Objekte des Backup-Speichers und der Quarantäne gespeichert werden (dieser Parameter kann nur über die Befehlszeile geändert werden).

Nach Ablauf des angegebenen Zeitraums oder bei Erreichen der maximalen Backup-Größe löscht die Anwendung 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.

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 Verwaltungskonsole (**Erweitert** → **Speicher** → **Backup**) und in der Web Console (**Vorgänge** → **Speicher** → **Backup**) verfügbar. Sie können die Eigenschaften von Dateien anzeigen, die sich in den Backup-Speichern der geschützten Geräten befinden, und Dateien aus diesen löschen. Kaspersky Security Center kopiert keine Dateien vom Backup auf den Administrationsserver; alle Dateien werden im Backup auf geschützten Geräten abgelegt. Die Dateiwiederherstellung wird auf einem geschützten Gerät durchgeführt.

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.

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.

Backup-Einstellungen in der Web Console konfigurieren

In der Web Console können Sie die Backup-Einstellungen in den Richtlinieneigenschaften (**Programmeinstellungen** → **Allgemeine Einstellungen** → **Berichte und Speicher**) und in den Eigenschaften des verwalteten Geräts (**Assets (Geräte)** → **Verwaltete Geräte** → Link <device name> → Registerkarte **Programme** → Link <Kaspersky Endpoint Security application name> → Registerkarte **Programmeinstellungen** → Abschnitt **Speichereinstellungen**) verwalten.

Die Backup-Einstellungen in den Richtlinieneigenschaften der Web Console werden in Anhang 5 beschrieben.

Die Backup-Einstellungen in den Eigenschaften des verwalteten Geräts werden in der folgenden Tabelle beschrieben.

Backup-Einstellungen in Geräteeigenschaften

Parameter	Description
Objekte nicht länger speichern als (Tage)	Eingabefeld zur Angabe des Zeitraums für das Speichern von Objekten im Backup. Zulässige Werte: 1 – 10000. Wenn kein Häkchen gesetzt wurde, ist der Zeitraum der Speicherung der Objekte im Backup unbegrenzt. Standardwert: 30.
Größe des Backup-Speichers begrenzen auf (MB)	Eingabefeld zur Angabe der maximalen Backup-Größe (in Megabyte). Wenn kein Häkchen gesetzt wurde, ist die Größe des Backup-Speichers unbegrenzt. Standardwert: 1024.

Backup-Einstellungen in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie Quarantäne-Einstellungen in den Richtlinieneigenschaften (Verwalten von Richtlinien in der Verwaltungskonsole, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Allgemeine Einstellungen** → **Speichereinstellungen**) und in den Eigenschaften verwalteter Geräte (**Verwaltete Geräte** → Registerkarte **Geräte** → Fenster mit den Geräteeigenschaften → Abschnitt **Anwendungen** → 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 – 999999. Wenn kein Häkchen gesetzt wurde, ist die Größe des Backup-Speichers unbegrenzt. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Konfigurieren der Backup-Einstellungen über die Befehlszeile

Über die Befehlszeile können Sie die Backup-Einstellungen mithilfe der Optionen `BackupDaysToLive`, `BackupSizeLimit` und `QuarantineBackupFolder` in den allgemeinen Anwendungseinstellungen konfigurieren.

Sie können den Wert von Parametern mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen 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 – 999999 0 – Die Größe des Backups ist nicht begrenzt. Standardwert: 0.
`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.

Verwendung von Objekten im Backup über die Befehlszeile

Über die Befehlszeile können Sie mit Befehlen zur Verwaltung des Backups die folgenden Aktionen mit Backup-Objekten ausführen:

- Informationen zu Backup-Objekten anzeigen.
- Alle oder nur bestimmte Objekte aus dem Backup löschen.
- Objekte aus dem Backup wiederherstellen.

Die Wiederherstellung infizierter Objekte kann zu einer Infektion des Geräts führen.

Informationen zu Backup-Objekten anzeigen

Um Informationen zu Backup-Objekten anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control -B --query ["<Filterbedingungen>"] [-n <Anzahl>] [--json]
```

wobei:

- Mit `<Filterbedingungen>` werden ein oder mehrere logische Ausdrücke im Format `<Feld> <Vergleichsoperation> '<Wert>'` angegeben, die mit dem logischen Operator `and` kombiniert werden, um Abfrageergebnisse einzuschränken. Wenn Sie keine Filterbedingungen angeben, zeigt die Anwendung Informationen zu allen Backup-Objekten an.
- `<Anzahl>` – Anzahl der letzten Objekte aus dem Speicher, deren Informationen ausgegeben werden. 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.

Objekte aus dem Backup wiederherstellen

So stellen Sie ein Objekt unter dem ursprünglichen Namen am ursprünglichen Speicherort wieder her:

```
kesl-control -B --restore <Objekt-ID>
```

Wobei gilt: < `Objekt-ID` > ist die numerische ID, welche die Anwendung dem Objekt zugewiesen hat, als es im Backup abgelegt wurde.

So stellen Sie ein Objekt unter einem neuen Namen in einem angegebenen Verzeichnis wieder her:

```
kesl-control -B --restore <Objekt-ID> --file <Dateipfad>
```

wobei `--file <Dateipfad>` der neue Name der Datei und der Pfad zu dem Verzeichnis ist, in dem Sie die Datei speichern möchten. Wenn das angegebene Verzeichnis nicht existiert, wird es von der Anwendung 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.

Bestimmte Objekte aus dem Backup löschen

Um ausgewählte Objekte aus dem Backup zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control -B --mass-remove --query "<Filterbedingungen>"
```

Dabei steht < `Filterbedingungen` > für einen oder mehrere logische Ausdrücke im Format < `Feld` > < `Vergleichsoperator` > '< `Wert` >', die mithilfe des logischen Operators `and` kombiniert werden, um die Ergebnisse einzuschränken.

Beispiele:
Um das Objekt mit ID=15 zu löschen:

```
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

So löschen Sie Objekte, deren Namen oder Pfade "test" enthalten:

```
kesl-control -B --mass-remove --query "FileName like '%test%'"
```

Um alle Objekte aus dem Backup zu löschen, führen Sie den folgenden Befehl aus:

```
kesl-control -B --mass-remove
```

Integration mit Detection and Response

Kaspersky Detection and Response-Lösungen sind Sicherheitssysteme zur Erkennung komplexer Bedrohungen und Angriffsindikatoren auf verschiedenen Ebenen einer Unternehmensinfrastruktur. Die Lösungen Detection and Response liefern Ihnen Informationen über erkannte Bedrohungen und ermöglichen Ihnen, Reaktionsmaßnahmen zu verwalten.

Kaspersky Endpoint Security kann mit den folgenden Lösungen Detection and Response von Kaspersky interagieren:

- Kaspersky Endpoint Detection and Response Expert (on-premise), basierend auf der Open Single Management Platform (OSMP). Die Integration erfolgt durch Kaspersky Endpoint Security als Komponente von Endpoint Detection and Response Expert (on-premise) (im Weiteren auch *EDR Expert (on-premise)*).
- 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 Weiteren auch *EDR Expert (On-Premise)*).
  - 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*).

Wenn Sie die Anwendung "Kaspersky Endpoint Security" im Modus als Endpoint Detection and Response Agent verwenden, wird nur die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) auf Basis der Open Single Management Platform (OSMP) und mit den Komponenten "Kaspersky Endpoint Detection and Response" und "Kaspersky Network Detection and Response" auf Basis der Kaspersky Anti Targeted Attack Platform unterstützt.

Im Rahmen der Integration von Kaspersky Endpoint Security mit den Lösungen Kaspersky Managed Detection and Response und Kaspersky Anti Targeted Attack Platform kann im systemd-Protokoll eine große Anzahl an Ereignissen eingetragen werden. Wenn Sie das Eintragen der Audit-Ereignisse in systemd deaktivieren wollen, müssen Sie den Socket systemd-journald-audit deaktivieren und das Betriebssystem neu starten.

So deaktivieren Sie den Socket systemd-journald-audit:

```
systemctl stop systemd-journald-audit.socket

systemctl disable systemd-journald-audit.socket

systemctl mask systemd-journald-audit.socket
```

Die Konfiguration des Dienstes "auditd" ist auf dem Betriebssystem SintezM-Client standardmäßig gegen Änderungen gesperrt, d. h. sie befindet sich im Ausführungsmodus `enabled 2`. Damit die Komponente "Verhaltensanalyse" bei einer Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response und Kaspersky Anti Targeted Attack Platform ordnungsgemäß funktioniert, müssen Sie in den Konfigurationsdateien den Ausführungsmodus von auditd in den Modus ohne Sperrung der Konfiguration (d. h. `enabled 1`) ändern und anschließend einen Neustart des Betriebssystems durchführen.

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-premise) vor

Über die Reaktionsmaßnahmen auf Befehle von Detection and Response

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 einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response wird die Netzwerkisolation in der entsprechenden Detection and Response-Lösung aktiviert und 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 einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response wird die Aufgabe erstellt und von der entsprechenden Detection and Response-Lösung 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 einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response wird die Reaktionsmaßnahme von der entsprechenden Detection and Response-Lösung bestimmt. 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 einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) und mit Kaspersky Endpoint Detection and Response (KATA) wird die Reaktionsmaßnahme von der entsprechenden Detection and Response-Lösung bestimmt. 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 einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) und mit Kaspersky Endpoint Detection and Response (KATA) wird die Reaktionsmaßnahme von der entsprechenden Detection and Response-Lösung bestimmt.

  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 einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response wird die Aufgabe erstellt und von der entsprechenden Detection and Response-Lösung 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 einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA) wird die Aufgabe in der entsprechenden Detection and Response-Lösung erstellt und gestartet.

  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 einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response wird die Aufgabe erstellt und von der entsprechenden Detection and Response-Lösung 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 einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response wird die Aufgabe erstellt und von der entsprechenden Detection and Response-Lösung 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.

- Erkennen 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.

  Bei einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA) wird die Aufgabe zur IOC-Untersuchung auf dem Gerät mit installiertem Kaspersky Endpoint Security in der entsprechenden Detection and Response-Lösung erstellt und gestartet.

  Bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum wird die IOC-Untersuchung mithilfe der Aufgabe zur IOC-Untersuchung durchgeführt (*IOC Scan*). Sie können die Aufgabe zur IOC-Untersuchung manuell erstellen.

- 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 zur YARA-Untersuchung auf einem Gerät mit installiertem Kaspersky Endpoint Security wird von Kaspersky Endpoint Detection and Response Expert (on-premise) erstellt und ausgeführt.

- Ausführungsprävention

  Bei einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Endpoint Detection and Response Optimum können Sie die Anwendung der Regeln für die Ausführungsprävention für Objekte aktivieren. Kaspersky Endpoint Security blockiert den Start von Objekten oder das Öffnen von Dokumenten entsprechend den Kriterien der Verbotsregel.

  Bei einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA) erhält die Anwendung die Regeln zur Ausführungsprävention von diesen entsprechenden Lösungen.

  Bei der Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie die Regeln der Ausführungsprävention für Objekte in der Web Console konfigurieren.

- Forensische Sammlung.

  Bei einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) können Sie digitale Daten erfassen, die der bei Untersuchung von Fällen der 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 in Kaspersky Endpoint Detection and Response Expert (on-premise) erstellt und gestartet.

Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise)

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).

Bei der Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) kann Kaspersky Endpoint Security die folgenden Funktionen ausführen:

- Informationen zu Ereignissen auf Geräten (Telemetriedaten) an Server zum Sammeln von Telemetriedaten auf Basis der OSMP-Plattform (im Weiteren auch *OSMP-Telemetrieserver*) senden. Kaspersky Endpoint Security sendet neben Überwachungsdaten zu Prozessen, offenen Netzwerkverbindungen und geänderten Dateien auch Daten zu den von der Anwendung erkannten Bedrohungen und deren Verarbeitungsergebnissen an den Telemetrieserver.
- Reaktionsmaßnahmen zur Gewährleistung der Sicherheitsfunktionen ausführen, die über Befehle von einem Server für Reaktionsmaßnahmen auf Basis der OSMP-Plattform (im Weiteren auch *OSMP-Reaktionsserver*) empfangen wurden.

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).

Bei der Integration mit 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. Um die Sicherheit dieser Verbindung zu gewährleisten, werden die folgenden, vom den OSMP-Servern ausgestellten Zertifikate verwendet:

- Serverzertifikat. Die Verbindung wird mit dem TLS-Zertifikat des Servers verschlüsselt. Sie können die Sicherheit der Verbindung erhöhen, indem Sie in Kaspersky Endpoint Security die Überprüfung des Serverzertifikats aktivieren. Fügen Sie dazu das Serverzertifikat hinzu, bevor Sie die Integration mit der Lösung Kaspersky Endpoint Detection and Response Expert (on-premise) aktivieren.

- Client-Zertifikat. Dieses Zertifikat dient dem zusätzlichen Schutz der Verbindung durch die Zwei-Wege-Authentifizierung (bei der Überprüfung der Geräte mit installiertem Kaspersky Endpoint Security durch die OSMP-Server). Mehrere Geräten können dasselbe Client-Zertifikat verwenden. Standardmäßig überprüft der Server keine Client-Zertifikate, es kann aber auf Seite von Kaspersky Endpoint Detection and Response Expert (on-premise) die Zwei-Wege-Authentifizierung aktiviert werden. In diesem Fall müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen von EDR Expert (on-premise) aktivieren und ein Client-Zertifikat hinzufügen (ein Crypto-Container mit einem Zertifikat und einem privaten Schlüssel).

Die Zertifikate zum Absichern der Verbindungen mit den OSMP-Servern werden vom Administrator der OSMP-Plattform bereitgestellt.

Wenn in den allgemeinen Einstellungen von Kaspersky Endpoint Security die Verwendung eines Proxyservers konfiguriert ist, wird dieser für die Verbindung zu OSMP-Servern verwendet.

Um die Funktionalität von Endpoint Detection and Response Expert (on-premise) zu verwenden, müssen Sie die Komponente EDR Expert (on-premise) aktivieren. Wenn von der Hauptlizenz, unter welcher Sie Kaspersky Endpoint Security verwenden, die Funktionen von Kaspersky Endpoint Detection and Response Expert (on-premise) nicht abgedeckt werden, müssen Sie für diese Funktionen eine separate Lizenz erwerben und den Lizenzschlüssel für EDR Expert (on-premise) zur Anwendung hinzufügen.

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

Die Integration mit Endpoint Detection and Response Expert (on-premise) umfasst die folgenden Schritte:

1. **Aktivieren der erforderlichen Komponenten von Kaspersky Endpoint Security**

   Die Komponente EDR Expert (on-premise) kann Daten aus den folgenden Komponenten verwenden:

   - Schutz vor bedrohlichen Dateien.
   - Schutz vor Netzwerkbedrohungen.
   - Schutz vor Web-Bedrohungen.
   - Schutz vor Verschlüsselung.
   - Programmkontrolle.
   - Gerätekontrolle.
   - Überwachung der Systemintegrität.

Um die Anwendung Kaspersky Endpoint Security vollständig in Kaspersky Endpoint Detection and Response Expert (on-premise) zu integrieren, müssen Sie die Komponente Verhaltensanalyse aktivieren. Bei deaktivierter Verhaltensanalyse werden keine erforderlichen Telemetriedaten übertragen (mit Ausnahme von Synchronisierungsanfragen und Daten zu erkannten Bedrohungen anderer Schutzkomponenten).

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.

2. **Aktivieren der von EDR Expert (on-premise)**

   Stellen Sie sicher, dass eine der folgenden Bedingungen erfüllt ist:

   - Sie verwenden Kaspersky Endpoint Security unter einer Lizenz, welche die Funktionalitäten von Kaspersky Endpoint Detection and Response Expert (on-premise) abdeckt.
   - Sie haben eine separate Lizenz zur Nutzung der Funktionalitäten von Kaspersky Endpoint Detection and Response Expert (on-premise) erworben und einen Lizenzschlüssel für EDR Expert (on-premise) zur Anwendung hinzugefügt.

     Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, wird der Lizenzschlüssel zum Aktivieren zusätzlicher Funktionen auf der SVM hinzugefügt.

3. **Aktivieren der Komponente EDR Expert (on-premise)**

   Die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) ist standardmäßig deaktiviert. Um die Integration zu aktivieren, müssen Sie die EDR Expert (on-premise) aktivieren und dessen Einstellungen konfigurieren.

   - Über die Kaspersky Security Center Web Console
   - Über die Befehlszeile

   Das Konfigurieren der Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) in der Verwaltungskonsole von Kaspersky Security Center wird nicht unterstützt.

   Für die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) müssen Sie in den Einstellungen der Komponente EDR Expert (on-premise) den Integrationsmodus *EDR Expert (OSMP)* auswählen. Wenn Sie die Web Console verwenden, wählen Sie **Endpoint Detection and Response Expert (Version 8.0 oder höher)** in den Richtlinieneinstellungen aus. Wenn Sie die Befehlszeile verwenden, geben Sie in den Aufgabeneinstellungen den Parameter `Mode=EDRExpertOnPrem` an. Um die Integration mit Kaspersky Endpoint Detection and Response Expert (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 Funktion zur Ausführungsprävention verwenden möchten, können Sie die Regeln zur Ausführungsprävention für Objekte in EDR Expert (on-premise) aktivieren.

Sie können den Status der Komponente EDR Expert (on-premise) überprüfen:

- Unter Verwendung des *Berichts über den Status der Programmkomponenten* in der Web Console.

  Weitere Informationen zum Umgang mit Berichten finden Sie in der Hilfe zu Kaspersky Security Center.

- In den Eigenschaften der Web Console (**Assets (Geräte)** → **Verwaltete Geräte** → Link <Name des Geräts> → **Anwendungen** → Link <Name von Kaspersky Endpoint Security> → **Allgemein** → **Komponenten**).

- In der Befehlszeile durch Ausführen des folgenden Befehls: `kesl-control --app-info`.

So bereiten Sie ein Referenzabbild für die korrekte Integration mit EDR Expert (on-premise) 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 Referenzabbild für die korrekte Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) 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.

Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) in der Web Console einrichten

In der Web Console können Sie die Komponente EDR Expert (on-premise) aktivieren oder deaktivieren und in den Richtlinieneigenschaften die Einstellungen für die Integration der Anwendung Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Expert (on-premise) verwalten (**Programmeinstellungen** → **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response Expert (on-premise)**).

Für die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) müssen Sie die Komponente "EDR Expert (on-premise)" aktivieren und die Option **Endpoint Detection and Response Expert (Version 8.0 und höher)** auswählen (d. h. den Integrationsmodus EDR *Expert (OSMP)*).

Für die Integrationsparameter von Kaspersky Endpoint Detection and Response Expert (on-premise) können Sie benutzerdefinierte Werte in verschachtelten Richtlinien auf Hierarchieebene festlegen, selbst wenn alle anderen Richtlinienparameter vererbt werden. Wenn die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) in der übergeordneten Richtlinie aktiviert und die Vererbung von Einstellungen in der untergeordneten Richtlinie aktiviert ist, werden die Integrationseinstellungen in der untergeordneten Richtlinie standardmäßig ebenfalls vererbt und können nicht geändert werden. Um eigene Integrationseinstellungen zu konfigurieren, wählen Sie in der Dropdown-Liste **Benutzerdefinierte Verbindungseinstellungen verwenden** aus. Die Parameter für die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) können geändert werden.

Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) über die Befehlszeile einrichten

Über die Befehlszeile können Sie die Integration von Kaspersky Endpoint Security mit der Lösung Kaspersky Endpoint Detection and Response Expert (on-premise) mithilfe der vordefinierten Aufgabe *Kaspersky Endpoint Detection and Response Expert (on-premise) (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 (OSMP)*-Integrationsmodus auswählen und die Integrationseinstellungen nach Bedarf verwalten.

Sie können Einstellungen für die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) konfigurieren, indem Sie die Einstellungen der vordefinierten Aufgabe ändern.

Standardmäßig wird die Aufgabe *Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise)* nicht gestartet. Sie können diese Aufgabe manuell starten und anhalten.

Mithilfe der Befehle zur Verwaltung von EDR Expert (on-premise) können Sie Zertifikate verwalten, die zur Verbindung mit OSMP-Servern verwendet werden.

Parameter für die Integration mit Endpoint Detection and Response Expert (on-premise)

In der folgenden Tabelle werden die Einstellungen der vordefinierten Aufgabe *„Integration in Kaspersky Endpoint Detection and Response Expert (on-premise) (KATAEDR)“* beschrieben, die Sie bei der Integration in Kaspersky Endpoint Detection and Response Expert (on-premise) verwalten können.

Diese Aufgabe ermöglicht Ihnen außerdem die Konfiguration der Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA). Um Kaspersky Endpoint Detection and Response Expert (on-premise) zu integrieren, müssen Sie in den Aufgabenparametern den Integrationsmodus *EDR Expert (OSMP)* (Parameter `Mode=EDRExpertOnPrem`) auswählen.

Parameter für die Integration mit Endpoint Detection and Response Expert (on-premise)

Parameter	Description	Wert
`Mode`	Modus der Integration. Bei einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) kommuniziert 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` – Integration im Modus EDR Expert (OSMP). Erlaubt die Integration mit 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 auf der Seite des OSMP-Reaktionsservers aktiviert ist, müssen Sie vor dem Aufgabenstart die Zwei-Wege-Authentifizierung in den Einstellungen der Aufgabe *Integration mit Kaspersky Endpoint Detection and Response (on-premise)* aktivieren und ein Client-Zertifikat hinzufügen.	`Ja` 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`	Aktivieren und Deaktivieren des Sendens von Daten über Ereignisse auf Geräten (Telemetriedaten) an den OSMP-Telemetrieserver.	`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.		
`Adresse`	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.		

Parameter	Description	Wert
`UseClientPinnedCertificate`	Aktivieren und Deaktivieren der Zwei-Wege-Authentifizierung, um die Verbindung zum OSMP-Telemetrieserver zusätzlich abzusichern. Wenn die Zwei-Wege-Authentifizierung auf der Seite des OSMP-Telemetrieservers aktiviert ist, müssen Sie vor dem Aufgabenstart die Zwei-Wege-Authentifizierung in den Einstellungen der Aufgabe *Integration mit Kaspersky Endpoint Detection and Response (on-premise)* aktivieren und ein Client-Zertifikat hinzufügen.	`Ja` 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`	Aktiviert oder deaktiviert das ausschließliche Senden von Telemetriedaten, die mit einem Angriffsindikator versehen sind (Indicator of Attack, IOA). Ein *IOA* beschreibt verdächtiges Verhalten von Objekten in der IT-Infrastruktur einer Organisation, das auf einen gezielten Angriff hindeuten kann.	`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.		
`Adresse`	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`	Begrenzung der Anzahl der an den OSMP-Telemetrieserver 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 OSMP-Servern 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 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 <Datei> --server-type response
```

wobei `<Datei>` 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 <Datei> --server-type response
   ```

   wobei `<Datei>` der Pfad zum Crypto-Container (PFX-Archiv) ist, der das Client-Zertifikat und den privaten Schlüssel enthält.

2. Wenn der Crypto-Container durch ein Kennwort geschützt ist, geben Sie das Kennwort ein, wenn Sie dazu aufgefordert werden.

Das Client-Zertifikat wird verwendet, um die Verbindung zum OSMP-Server zusätzlich abzusichern, wenn die Überprüfung des Client-Zertifikats in den Einstellungen des OSMP-Servers aktiviert ist und in den Aufgabeneinstellungen der *Integration in Kaspersky Endpoint Detection and Response Expert (on-premise)* 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 <Datei> --server-type telemetry
```

wobei `<Datei>` 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 <Datei> --server-type telemetry
   ```

   wobei `<Datei>` der Pfad zum Crypto-Container (PFX-Archiv) ist, der das Client-Zertifikat und den privaten Schlüssel enthält.

2. Wenn der Crypto-Container durch ein Kennwort geschützt ist, geben Sie das Kennwort ein, wenn Sie dazu aufgefordert werden.

Das Client-Zertifikat wird verwendet, um die Verbindung zum OSMP-Server zusätzlich abzusichern, wenn die Überprüfung des Client-Zertifikats in den Einstellungen des OSMP-Servers aktiviert ist und in den Aufgabeneinstellungen der *Integration in Kaspersky Endpoint Detection and Response Expert (on-premise)* 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 Anti Targeted Attack Platform

Kaspersky Endpoint Security unterstützt die Kaspersky Anti Targeted Attack Platform, die darauf ausgelegt ist, die IT-Infrastruktur einer Organisation zu schützen und Bedrohungen wie Zero-Day-Angriffe, zielgerichtete Angriffe und Advanced Persistent Threats (im Folgenden auch "APT") rechtzeitig zu erkennen. 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. Im Rahmen der Integration mit Kaspersky Endpoint Detection and Response (KATA) kann Kaspersky Endpoint Security die folgenden Funktionen ausführen:
  - Daten über Ereignisse auf Geräten (Telemetriedaten) an den Server mit der Komponente "Central Node" übertragen, welcher die Interaktion mit Kaspersky Endpoint Detection and Response (KATA) gewährleistet (im Folgenden auch als *KATA-Server* bezeichnet). Kaspersky Endpoint Security sendet neben Überwachungsdaten zu Prozessen, offenen Netzwerkverbindungen und geänderten Dateien auch Daten zu den von der Anwendung erkannten Bedrohungen und zu den Verarbeitungsergebnissen dieser Bedrohungen an den Server mit der Central-Node-Komponente auf Basis der Kaspersky Anti Targeted Attack Platform
  - Ausführen von Reaktionsmaßnahmen, um die Sicherheitsfunktionen mittels der Befehle sicherzustellen, die von Kaspersky Anti Targeted Attack Platform übertragen wurden.

Die Integration mit Kaspersky Endpoint Detection and Response (KATA) Version 7.1 und niedriger wird unterstützt.

- Kaspersky 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 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. Bei der Integration von Kaspersky Endpoint Security mit Sandbox auf Basis der Kaspersky Anti Targeted Attack Platform sendet die Anwendung Dateien zur Untersuchung an einen Server mit Central-Node-Komponente, welche die Interaktion mit der Sandbox gewährleistet.

Die Integration mit Komponenten auf Basis der Kaspersky Anti Targeted Attack Platform wird durch die folgenden Komponenten von Kaspersky Endpoint Security gewährleistet:

- Komponente "Endpoint Detection and Response Expert (on-premise)" (im Weiteren auch *EDR Expert (on-premise)*).

  Beginnend mit Kaspersky Endpoint Security 12.4 für Linux wurde Endpoint Detection and Response (KATA) in Endpoint Detection and Response Expert (on-premise) umbenannt. Diese Komponente ermöglicht jetzt neben der Integration mit Kaspersky Endpoint Detection and Response (KATA) (eine Komponente der Kaspersky Anti Targeted Attack Platform) auch die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise).

- Komponente "Network Detection and Response (KATA)" (im Folgenden auch *NDR (KATA)* genannt).

- Komponente "*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.

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. Um die Sicherheit dieser Verbindung zu gewährleisten, werden die folgenden, von den Central-Node-Servern ausgestellten Zertifikate verwendet:

- Serverzertifikat. Die Verbindung wird mit dem TLS-Zertifikat des Servers verschlüsselt. Sie können die Sicherheit der Verbindung erhöhen, indem Sie in Kaspersky Endpoint Security die Überprüfung des Serverzertifikats aktivieren. Dazu müssen Sie das Zertifikat des Servers hinzufügen, bevor Sie die Integration mit der Kaspersky Anti Targeted Attack Platform-Lösung aktivieren.

- Client-Zertifikat. Dieses Zertifikat dient dem zusätzlichen Schutz der Verbindung durch die Zwei-Wege-Authentifizierung (bei der Überprüfung der Geräte mit installiertem Kaspersky Endpoint Security durch die Central-Node-Server). Mehrere Geräten können dasselbe Client-Zertifikat verwenden. Standardmäßig überprüft der Server keine Client-Zertifikate, aber die Zwei-Wege-Authentifizierung kann auf der Seite von Kaspersky Anti Targeted Attack Platform aktiviert werden. In diesem Fall müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen der Integration mit EDR Expert (on-premise), NDR (KATA) oder Sandbox aktivieren und ein Client-Zertifikat hinzufügen (ein Crypto-Container mit einem Zertifikat und einem privaten Schlüssel).

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.

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.

Um die Funktionen von Kaspersky Endpoint Detection and Response (KATA) verwenden zu können, müssen Sie EDR Expert (on-premise) aktivieren. Wenn von der Hauptlizenz, unter welcher Sie Kaspersky Endpoint Security verwenden, die Funktionen von Kaspersky Endpoint Detection and Response Expert (on-premise) nicht abgedeckt werden, müssen Sie für diese Funktionen eine separate Lizenz erwerben und den Lizenzschlüssel für EDR Expert (on-premise) zur Anwendung hinzufügen.

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

Die Integration mit den Komponenten von Kaspersky Endpoint Detection and Response (KATA) und Kaspersky Network Detection and Response (KATA) umfasst die folgenden Schritte:

1. **Aktivieren der erforderlichen Komponenten von Kaspersky Endpoint Security**

   Die Komponenten EDR Expert (on-premise) und NDR (KATA) können Daten verwenden, die von den folgenden Komponenten stammen:

   - Schutz vor bedrohlichen Dateien.
   - Schutz vor Netzwerkbedrohungen.
   - Schutz vor Web-Bedrohungen.
   - Schutz vor Verschlüsselung.
   - Programmkontrolle.
   - Gerätekontrolle.
   - Überwachung der Systemintegrität.

   Für eine vollständige Integration von Kaspersky Endpoint Security mit Kaspersky Anti Targeted Attack Platform muss die Komponente Verhaltensanalyse aktiviert sein. Bei deaktivierter Verhaltensanalyse werden keine erforderlichen Telemetriedaten übertragen (mit Ausnahme von Synchronisierungsanfragen und Daten zu erkannten Bedrohungen anderer Schutzkomponenten).

   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.

2. **Aktivieren der von EDR Expert (on-premise)**

Zur Integration mit Kaspersky Endpoint Detection and Response (KATA) müssen Sie EDR Expert (on-premise) aktivieren. Stellen Sie sicher, dass eine der folgenden Bedingungen erfüllt ist:

- Sie verwenden Kaspersky Endpoint Security unter einer Lizenz, welche die Funktionalitäten von Kaspersky Endpoint Detection and Response Expert (on-premise) abdeckt.
- Sie haben eine separate Lizenz zur Nutzung der Funktionalitäten von Kaspersky Endpoint Detection and Response Expert (on-premise) erworben und einen Lizenzschlüssel für EDR Expert (on-premise) zur Anwendung hinzugefügt.

  Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, wird der Lizenzschlüssel zum Aktivieren zusätzlicher Funktionen auf der SVM hinzugefügt.

Die Aktivierung von NDR (KATA) ist nicht erforderlich, da die Basislizenzen für Kaspersky Endpoint Security die Integration mit Kaspersky Network Detection and Response (KATA) beinhalten.

3. **Aktivieren der Komponente EDR Expert (on-premise)**

   Standardmäßig ist die Integration mit Kaspersky Endpoint Detection and Response (KATA) deaktiviert. Um die Integration zu aktivieren, müssen Sie die EDR Expert (on-premise) aktivieren und dessen Einstellungen konfigurieren.

   - Über die Kaspersky Security Center Web Console
   - Mittels der Verwaltungskonsole von Kaspersky Security Center.
   - Über die Befehlszeile

   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 und niedriger)** aus. Wenn Sie die Befehlszeile verwenden, geben Sie in den Aufgabeneinstellungen den Parameter `Mode=EDRKATA` an. 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 Funktion zur Ausführungsprävention verwenden möchten, können Sie die Regeln zur Ausführungsprävention für Objekte in EDR Expert (on-premise) aktivieren.

4. **Aktivieren der Komponente NDR (KATA):**

   Standardmäßig ist die Integration mit Kaspersky Network Detection and Response (KATA) deaktiviert. Um die Integration zu aktivieren, müssen Sie NDR (KATA) aktivieren und dessen Einstellungen konfigurieren.

   - Über die Kaspersky Security Center Web Console
   - Mittels der Verwaltungskonsole von Kaspersky Security Center.
   - Über die Befehlszeile

Sie können den Ausführungsstatus der Komponenten EDR Expert (on-premise) und NDR (KATA) wie folgt überprüfen:

- Unter Verwendung des *Berichts über den Status der Programmkomponenten* in der Web Console.

  Weitere Informationen zum Umgang mit Berichten finden Sie in der Hilfe zu Kaspersky Security Center.

- In den Eigenschaften der Web Console (**Assets (Geräte)** → **Verwaltete Geräte** → Link <Name des Geräts> → **Anwendungen** → Link <Name von Kaspersky Endpoint Security> → **Allgemein** → **Komponenten**).
- In der Befehlszeile durch Ausführen des folgenden Befehls: `kesl-control --app-info`.

Integration mit Kaspersky Endpoint Detection and Response (KATA) in der Web Console einrichten

In der Web Console können Sie in den Richtlinieneigenschaften die Einstellungen für die Integration von Kaspersky Endpoint Detection and Response (KATA) verwalten (**Programmeinstellungen** → **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response Expert (on-premise)**).

Für die Integration mit Kaspersky Endpoint Detection and Response Expert (KATA) müssen Sie die Komponente "EDR Expert (on-premise)" aktivieren und die Option **Endpoint Detection and Response Expert (Version 7.1 und niedriger)** auswählen (d. h. den Integrationsmodus *EDR (KATA)*).

Um den Wert der Einstellung **Maximale Verzögerung beim Senden von Ereignissen (Sek.)**, der unter **Datenübertragungseinstellungen** für die Komponente Endpoint Detection and Response Expert (KATA) in der Richtlinie in der Web Console festgelegt ist, zu übernehmen, müssen Sie in den Richtlinieneigenschaften die „Schlösser" für die Einstellungsgruppen **Datenübertragungseinstellungen** und **Anfragedrosselung** schließen. Um das lokale Ändern der Einstellung `MaximumDataTransferTime` auf dem Gerät zu ermöglichen, müssen Sie im Abschnitt `[EventTransferSettings]` für die Aufgabe KATAEDR im Modus EDR (KATA) in den Richtlinieneigenschaften die „Schlösser" für die Einstellungsgruppen **Datenübertragungseinstellungen** und **Anfragedrosselung** entsperren.

Integration mit Kaspersky Endpoint Detection and Response (KATA) in der Verwaltungskonsole einrichten

In der Verwaltungskonsole können Sie die Komponente EDR Expert (on-premise) aktivieren oder deaktivieren und in den Richtlinieneigenschaften die Einstellungen für die Integration von Kaspersky Endpoint Security mit der Komponente Kaspersky Endpoint Detection and Response (KATA) verwalten (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Detection and Response** → **EDR Expert (on-premise)**).

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 wurde (d. h. der Integrationsmodus "EDR Expert (OSMP)"), wird in der Verwaltungskonsole eine Warnung angezeigt, das die Parameter zur Integration mit Kaspersky Endpoint Detection and Response (KATA) nicht verfügbar sind. Sie können in der Web Console den Integrationsmodus ändern.

Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA)

Parameter	Description
Endpoint Detection and Response Expert (on-premise) aktivieren	Das Kontrollkästchen aktiviert oder deaktiviert die Komponente "EDR Expert (on-premise)", welche die Integration mit Kaspersky Endpoint Detection and Response (KATA) gewährleistet. Die Komponente ist standardmäßig deaktiviert.
Ausführungsprävention für Objekte aktivieren	Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung der Regeln der Ausführungsprävention der Komponente "EDR Expert (on-premise)".
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 Verbindungseinstellungen mit den KATA-Servern konfigurieren.

Einstellungen für die Verbindung mit den KATA-Servern

Parameter	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`.

Parameter	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 bidirektionale 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. Wenn das Archiv durch ein Kennwort geschützt ist, geben Sie das Kennwort in das Feld **Kennwort des Crypto-Containers** ein. • **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.
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 Endpoint Detection and Response (KATA) über die Befehlszeile einrichten

Über die Befehlszeile können Sie die Integration von Kaspersky Endpoint Security mit der Komponente Kaspersky Endpoint Detection and Response (KATA) mithilfe der *Integration mit Kaspersky Endpoint Detection and Response (KATA) (KATAEDR)*, einer vordefinierten Aufgabe, verwalten.

Diese Aufgabe ermöglicht Ihnen außerdem die Konfiguration der Integrationseinstellungen mit der Lösung "Kaspersky Endpoint Detection and Response Expert (on-premise)". Für die Integration mit Kaspersky Endpoint Detection and Response (KATA) müssen Sie in den Aufgabeneinstellungen den *EDR (KATA)*-Integrationsmodus 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 mit Kaspersky Endpoint Detection and Response Expert (on-premise)* nicht gestartet. Sie können diese Aufgabe manuell starten und anhalten.

Mithilfe der Befehle zur Verwaltung von EDR Expert (on-premise) können Sie Zertifikate verwalten, die zur Verbindung mit KATA-Servern verwendet werden.

Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA)

Die folgende Tabelle beschreibt die Parameter der vordefinierten Aufgabe *Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) (KATAEDR)*, die Sie bei der Integration mit Kaspersky Endpoint Detection and Response (KATA) konfigurieren können.

Diese Aufgabe ermöglicht Ihnen außerdem die Konfiguration der Integrationseinstellungen mit der Lösung "Kaspersky Endpoint Detection and Response Expert (on-premise)". 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 einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) kommuniziert 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` – Integration im Modus EDR Expert (OSMP). Erlaubt die Integration mit 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 auf der Seite des KATA-Servers aktiviert ist, müssen Sie vor dem Aufgabenstart die Zwei-Wege-Authentifizierung in den Einstellungen der Aufgabe *Integration mit Kaspersky Endpoint Detection and Response (on-premise)* aktivieren und ein 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`	Aktivieren und Deaktivieren des Sendens von Daten über Ereignisse auf Geräten (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.		
`Adresse`	Adresse des KATA-Servers. Sie können die IP-Adresse (IPv4 oder IPv6) oder den vollqualifizierten Domänennamen (FQDN) des Servers angeben. Um sicherzustellen, dass die Kommunikation mit dem 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 <Datei>
```

wobei `<Datei>` 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 <Datei>
   ```

   wobei `<Datei>` der Pfad zum Crypto-Container (PFX-Archiv) ist, der das Client-Zertifikat und den privaten Schlüssel enthält.

2. Wenn der Crypto-Container durch ein Kennwort geschützt ist, geben Sie das Kennwort ein, wenn Sie dazu aufgefordert werden.

Das Client-Zertifikat wird 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-premise)* `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) in der Web Console einrichten

In der Web Console können Sie die Einstellungen für die Integration mit Kaspersky Network Detection and Response (KATA) in den Richtlinieneigenschaften verwalten (**Programmeinstellungen** → **Konfiguration der integrierten Agenten** → **Network Detection and Response (KATA)**).

Um den Wert der Einstellung **Maximale Verzögerung beim Senden von Ereignissen (Sek.)**, der unter **Datenübertragungseinstellungen** für die Komponente Network Detection and Response (KATA) in der Richtlinie in der Web Console angegeben wurde, anzuwenden, müssen Sie in den Richtlinieneigenschaften die „Schlösser" für die Einstellungsgruppen **Datenübertragungseinstellungen** und **Anforderungsdrosselung** schließen. Um die lokale Änderung der Einstellung `MaximumDataTransferTime` auf dem Gerät im Abschnitt `[EventTransferSettings]` für die Aufgabe KATANDR zu erlauben, müssen Sie in den Richtlinieneigenschaften die „Schlösser" für die Einstellungsgruppen **Datenübertragungseinstellungen** und **Anforderungsdrosselung** öffnen.

Integration mit Kaspersky Network Detection and Response (KATA) in der Verwaltungskonsole einrichten

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 Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) 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 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. Dort können Sie die allgemeinen Einstellungen für die Verbindung mit NDR-Servern konfigurieren, ein Serverzertifikat hinzufügen und die Zwei-Wege-Authentifizierung für die Verbindung mit NDR-Servern konfigurieren.
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.

Konfiguration der Verbindung mit NDR-Servern

Die Tabelle enthält eine Liste der Parameter für die Verbindung mit 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:

- Parameter für eine Verbindung 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 zu NDR-Servern konfigurieren

In diesem Fenster können Sie die allgemeinen Einstellungen für Verbindungen mit NDR-Servern konfigurieren.

Einstellungen der Verbindung mit 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.

Parameter	Description
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 Zwei-Wege-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. Wenn das Archiv durch ein Kennwort geschützt ist, geben Sie das Kennwort in das Feld **Kennwort des Crypto-Containers** ein. • **Löschen** – Entfernt ein zuvor hinzugefügtes Client-Zertifikat. Die Schaltfläche wird nur angezeigt, wenn ein Client-Zertifikat hinzugefügt wurde.

Konfiguration der Datenübertragung an die NDR-Server

In diesem Fenster können Sie die Einstellungen für die Datenübertragung an die NDR-Server konfigurieren.

Einstellungen für die 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 Kaspersky Network Detection and Response (KATA) über die Befehlszeile einrichten

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 diese Aufgabe manuell starten und anhalten.

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)* 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.		
`Adresse`	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`	Prozentuale Überschreitung der Ereignisbegrenzung. 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 <Datei>
```

wobei `<Datei>` 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 <Datei>
   ```

   wobei `<Datei>` der Pfad zum Crypto-Container (PFX-Archiv) ist, der das Client-Zertifikat und den privaten Schlüssel enthält.

2. Wenn der Crypto-Container durch ein Kennwort geschützt ist, geben Sie das Kennwort ein, wenn Sie dazu aufgefordert werden.

Das Client-Zertifikat wird verwendet, um die Verbindung zum 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

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.

Kaspersky Endpoint Security kann sowohl mit Sandbox auf Basis der Open Single Management Platform (OSMP) als auch mit Sandbox auf Basis der Kaspersky Anti Targeted Attack Platform interagieren. Kaspersky Endpoint Security kommuniziert mit Sandbox über einen *Sandbox-Server*. Dies ist je nach Plattform ein OSMP-Server oder ein Server mit Central-Node-Komponente.

Die Integration mit Sandbox erfolgt über die *Sandbox*-Komponente von Kaspersky Endpoint Security.

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. Um die Sicherheit dieser Verbindung zu gewährleisten, werden die folgenden, vom OSMP- oder Central-Node-Server ausgestellten Zertifikate verwendet:

- Serverzertifikat. Die Verbindung wird mit dem TLS-Zertifikat des Servers verschlüsselt. Sie können die Sicherheit der Verbindung erhöhen, indem Sie in Kaspersky Endpoint Security die Überprüfung des Serverzertifikats aktivieren. Dazu müssen Sie das Zertifikat des Integrationsservers hinzufügen, bevor Sie die Integration mit Sandbox aktivieren.
- Client-Zertifikat. Dieses Zertifikat dient dem zusätzlichen Schutz der Verbindung durch die Zwei-Wege-Authentifizierung (bei der Überprüfung der Geräte mit installiertem Kaspersky Endpoint Security durch den OSMP- oder Central-Node-Server). Mehrere Geräten können dasselbe Client-Zertifikat verwenden. Standardmäßig überprüft der Server keine Client-Zertifikate, aber die Zwei-Wege-Authentifizierung kann auf der Seite der OSMP-Plattform oder von Kaspersky Anti Targeted Attack Platform aktiviert werden. In diesem Fall müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen der Sandbox-Komponente aktivieren und ein Client-Zertifikat hinzufügen (ein Crypto-Container mit einem Zertifikat und einem privaten Schlüssel).

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.

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.

Für das Versenden von Dateien und Verzeichnissen zur Untersuchung an die Sandbox stehen folgende Modi zur Verfügung:

- *Manuell*. In diesem Modus können Sie die Objekte per Befehl manuell oder über die grafische Oberfläche zur Untersuchung an die Sandbox versenden.
- *Nur automatisch*. Die Anwendung versendet die Objekte automatisch zur Untersuchung. Das manuelle Versenden von Objekten zur Untersuchung an die Sandbox ist nicht möglich.
- *Automatisch und manuell*. 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.

Die Integration mit Sandbox ist standardmäßig deaktiviert. Sie können die Sandbox-Komponente aktivieren und deaktivieren und die folgenden Integrationseinstellungen in der Web Console und über die Befehlszeile konfigurieren:

- Wählen Sie den Modus für das Versenden von Objekten (manuell, nur automatisch, automatisch und manuell) aus.
- Wählen Sie die Aktionen aus, die von der Anwendung bei Erkennung einer Bedrohung ausgeführt wird (im asynchronen Modus zum Versenden von Objekten an die Sandbox):
  - Datei mit dem erkannten Objekt löschen und Kopie der Datei in die Quarantäne verschieben.
  - Die Aufgabe zur Untersuchung wichtiger Bereiche starten. Standardmäßig untersucht die Anwendung den Speicher von Prozessen, den Kernel-Speicher, Bootsektoren, Autostart-Objekte und den Pfad zum erkannten Objekt.
  - Eine Aufgabe zur IOC-Untersuchung erstellen. Die Anwendung erstellt eine Aufgabe zur IOC-Untersuchung automatisch. Sie können den Startmodus der Aufgabe, den Untersuchungsbereich und die Aktion bei Erkennung eines IOCs konfigurieren (erkanntes Objekt löschen, Untersuchung wichtiger Bereiche ausführen).
- Allgemeine Einstellungen für die Verbindung mit den Sandbox-Servern konfigurieren.
- Zertifikate der Sandbox-Server hinzufügen oder entfernen.
- Die Zwei-Wege-Authentifizierung beim Herstellen einer Verbindung mit den Sandbox-Servern konfigurieren und Client-Zertifikate hinzufügen.

Integration mit Sandbox in Web Console konfigurieren

In der Web Console können Sie die Einstellungen zur Integration der Anwendung mit Sandbox in den Richtlinieneigenschaften konfigurieren (**Anwendungseinstellungen** → **Konfiguration der integrierten Agenten** → **Sandbox**).

Integration mit Sandbox über die Befehlszeile konfigurieren

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.

> Die Aufgabe *Integration mit Sandbox* kann nicht gestartet werden, wenn kein Serverzertifikat hinzugefügt wurde.

Wenn die Aufgabe *Integration mit Sandbox* ausgeführt wird, können Sie über die Befehlszeile Dateien zur Untersuchung an Sandbox senden.

Um Dateien zur Untersuchung an Sandbox zu senden, führen Sie den folgenden Befehl aus:

```
kesl-control [-X] --sandbox <Pfad>
```

wobei `<Pfad>` der Datei oder dem Verzeichnis entspricht, dass 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* festlegen können.

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`.

Parameter	Description	Wert
`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.
Der Abschnitt **[Servers.item_#]** enthält die Parameter des Sandbox-Servers.		
`Adresse`	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 <Datei>
```

wobei `<Datei>` der Pfad zur Datei ist, die das Serverzertifikat enthält.

Um ein Client-Zertifikat hinzuzufügen oder zu ersetzen:

1. Führen Sie den Befehl aus:

   ```
   kesl-control [-X] --add-sandbox-client-certificate <Datei>
   ```

   wobei `<Datei>` der Pfad zum Crypto-Container (PFX-Archiv) ist, der das Client-Zertifikat und den privaten Schlüssel enthält.

2. Wenn der Crypto-Container durch ein Kennwort geschützt ist, geben Sie das Kennwort ein, wenn Sie dazu aufgefordert werden.

Das Client-Zertifikat wird verwendet, um die Verbindung zum Sandbox-Server zusätzlich abzusichern, wenn die Überprüfung des Client-Zertifikats in den Einstellungen des Sandbox-Servers aktiviert ist und der Parameter `UseClientCertificate` in den Einstellungen der Aufgabe *Integration mit Sandbox* auf `yes` steht.

Um Informationen zum Zertifikat anzuzeigen, führen Sie den folgenden Befehl aus:

- Für ein Serverzertifikat:

  ```
  kesl-control [-X] --query-sandbox-server-certificate
  ```

- Für ein 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

Kaspersky Endpoint Detection and Response Optimum ist eine Lösung zum Schutz der IT-Infrastruktur eines Unternehmens vor Bedrohungen wie Exploits, Ransomware, dateilosen Angriffen (fileless attacks) und dem bösartigen Ausnutzen legitimer System-Tools zur Beschädigung von Geräten und Daten.

Kaspersky Endpoint Detection and Response Optimum überwacht und analysiert die Entwicklung einer Bedrohung und stellt zusätzlich dem Security Officer oder Administrator Informationen über einen potenziellen Angriff zur Verfügung, die für ein rechtzeitiges Ergreifen von Gegenmaßnahmen notwendig sind.

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.

Kaspersky Endpoint Security 12.4 für Linux ist mit Kaspersky Endpoint Detection and Response Optimum Version 3.1 kompatibel.

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.

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*).

Um die Funktionen von Kaspersky Endpoint Detection and Response Optimum verwenden zu können, müssen Sie die Komponente "EDR Optimum" aktivieren. Wenn von der Hauptlizenz, unter welcher Sie Kaspersky Endpoint Security verwenden, die Funktionen von Kaspersky Endpoint Detection and Response Optimum nicht abgedeckt werden, müssen Sie für diese Funktionen eine separate Lizenz erwerben und den Lizenzschlüssel für EDR Optimum zur Anwendung hinzufügen.

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

Die Integration mit Kaspersky Endpoint Detection and Response Optimum besteht aus den folgenden Schritten:

1. **Aktivieren der erforderlichen Komponenten von Kaspersky Endpoint Security**

   Stellen Sie sicher, dass die folgenden Komponenten von Kaspersky Endpoint Security aktiviert sind und einsatzbereit sind:

   - Schutz vor bedrohlichen Dateien.
   - Schutz vor Web-Bedrohungen.
   - Verhaltensanalyse.

   Sie können auch die Ausführungsprävention für Objekte aktivieren.

2. **Aktivieren der Tools zur Bedrohungsanalyse**

   Stellen Sie sicher, dass Kaspersky Security Network im Standard-Modus oder im erweiterten Modus aktiviert ist.

   Für eine optimale Ausführung von Kaspersky Endpoint Detection and Response Optimum wird es empfohlen, Kaspersky Security Network im erweiterten Modus zu verwenden.

3. **Aktivieren von EDR Optimum**

Stellen Sie sicher, dass eine der folgenden Bedingungen erfüllt ist:

- Sie verwenden Kaspersky Endpoint Security unter einer Lizenz, welche die Funktionalitäten von Kaspersky Endpoint Detection and Response Optimum abdeckt.
- Sie haben eine separate Lizenz zur Nutzung der Funktionalitäten von Kaspersky Endpoint Detection and Response Optimum erworben und einen Lizenzschlüssel für EDR Optimum zur Anwendung hinzugefügt.

  Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, wird der Lizenzschlüssel zum Aktivieren zusätzlicher Funktionen auf der SVM hinzugefügt.

4. **Installieren des Verwaltungs-Plug-ins 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.

5. **Aktivieren von EDR Optimum**

   EDR Optimum ist standardmäßig deaktiviert. Die Komponente aktivieren und deaktivieren, sowie deren Einstellungen konfigurieren, können Sie:

   - Mittels Web Console
   - Über die Befehlszeile

     Die Verwaltung von EDR Optimum über die Verwaltungskonsole von Kaspersky Security Center wird nicht unterstützt.

   Sie können den Ausführungsstatus von EDR Optimum wie folgt überprüfen:

   - Unter Verwendung des *Berichts über den Status der Programmkomponenten* in der Web Console.

     Die Komponente **Endpoint Detection and Response Optimum** wurde zur Liste der Komponenten von Kaspersky Endpoint Security hinzugefügt. Weitere Informationen zum Umgang mit Berichten finden Sie in der Hilfe zu Kaspersky Security Center.
   - In den Geräteeigenschaften in der Web Console.
   - Über die Befehlszeile

6. **Aktivieren der Übertragung von Daten 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.

Integration mit Kaspersky Endpoint Detection and Response Optimum aktivieren und deaktivieren

Aktivieren oder deaktivieren können Sie die Komponente "EDR Optimum":

- Mittels Web Console
- Über die Befehlszeile

Das Verwalten der Einstellungen für die Integration mit Kaspersky Endpoint Detection and Response Optimum über die Verwaltungskonsole wird nicht unterstützt.

Integration mit Kaspersky Endpoint Detection and Response Optimum in der Web Console aktivieren und deaktivieren

In der Web Console können Sie sowohl die Komponente "EDR Optimum" aktivieren und deaktivieren als auch die Integrationseinstellungen mit Kaspersky Endpoint Detection and Response Optimum konfigurieren:

- In den Richtlinieneigenschaften (**Anwendungseinstellungen** → **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response**)
- In den Eigenschaften verwalteter Geräte (**Assets (Geräte)** → **Verwaltete Geräte** → Link <Gerätename> → Registerkarte **Anwendungen** → Link <Name des Kaspersky Endpoint Security-Programms> → Registerkarte **Programmeinstellungen** → Abschnitt **Detection and Response** → **Endpoint Detection and Response Optimum**).

  Das Aktivieren und Deaktivieren von EDR Optimum ist in den Geräteeigenschaften nicht verfügbar, wenn das Gerät durch eine Richtlinie verwaltet wird ist.

Integrationseinstellungen mit Kaspersky Endpoint Detection and Response Optimum in den Geräteeigenschaften

Parameter	Description
Endpoint Detection and Response Optimum ist aktiviert/deaktiviert	Aktiviert oder deaktiviert die Komponente "EDR Optimum", die für die Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Optimum erforderlich ist. Der Schalter ist standardmäßig deaktiviert.
Netzwerkisolation	Über den Link **Einrichten der Gerätefreigabe**, wird das Fenster **Einstellung der Gerätefreigabe** geöffnet, in dem Sie die Dauer der Geräteblockierung konfigurieren können.
Ausnahmen	Der Link **Ausschlüsse konfigurieren** öffnet das Fenster Ausnahmen, in dem Sie die Ausnahmen für die Netzwerkisolation konfigurieren können.

Integration mit Kaspersky Endpoint Detection and Response Optimum über die Befehlszeile aktivieren und deaktivieren

Über die Befehlszeile können Sie die Funktionen von EDR Optimum mit dem Parameter `UseEdrOptimum` in den allgemeinen Anwendungseinstellungen aktivieren oder deaktivieren.

Sie können den Wert des Parameters mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen 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
```

Status der Integration mit Kaspersky Endpoint Detection and Response Optimum

Status der Integration in der Web Console anzeigen

Sie können den Status der Integration mit Kaspersky Endpoint Detection and Response Optimum in der Web Console auf folgende Weise anzeigen: Wechseln Sie zum Abschnitt **Assets (Geräte)** → **Verwaltete Geräte** → Link <Name des Geräts> → Registerkarte **Anwendungen** → <Name von Kaspersky Endpoint Security> → Registerkarte **Allgemein** → **Komponenten**.

Status der Integration über die Befehlszeile anzeigen

Sie können den Status der Integration mit Kaspersky Endpoint Detection and Response Optimum über die Befehlszeile anzeigen, indem Sie den Befehl `kesl-control --app-info` ausführen.

Statuswerte für die Integration

Für EDR Optimum wird einer der folgenden Statuswerte angezeigt:

- *Wird ausgeführt*.

Dieser Status wird angezeigt, wenn die folgenden Bedingungen gleichzeitig erfüllt sind:

- Es wurde ein Lizenzschlüssel hinzugefügt, der zur Ausführung von EDR Optimum erforderlich ist
- Das aktuelle Datum überschreitet nicht das Ablaufdatum der Lizenz
- Es ist mindestens eine der Komponenten von Kaspersky Endpoint Security aktiviert, die für die Funktion von EDR Optimum erforderlich sind
- Die Integration mit Kaspersky Endpoint Detection and Response Optimum ist auf dem Gerät aktiviert

- *Angehalten*.

  Dieser Status wird in folgenden Fällen angezeigt:

  - Die Integration mit Kaspersky Endpoint Detection and Response Optimum ist deaktiviert
  - Kaspersky Endpoint Security wurde angehalten

- *Von der Lizenz nicht unterstützt*.

  Dieser Status wird in folgenden Fällen angezeigt:

  - Das aktuelle Datum überschreitet das Ablaufdatum der Lizenz
  - Die aktuelle Lizenz beinhaltet keine Funktionalität für EDR Optimum

- *Fehler*.

  Dieser Status wird angezeigt, wenn die folgenden Bedingungen gleichzeitig erfüllt sind:

  - Das aktuelle Datum überschreitet nicht das Ablaufdatum der Lizenz
  - Beim Ausführen mindestens einer der Komponenten von Kaspersky Endpoint Security, die für den Betrieb von EDR Optimum erforderlich sind, ist ein Fehler aufgetreten

Informationen zur erkannten Bedrohung und möglichen Reaktionsmaßnahmen anzeigen

Um alle Informationen zu einer erkannten Bedrohung anzuzeigen und Maßnahmen zur Reaktion auf diese Bedrohung durchzuführen, können Sie das Fenster mit den Alarmdetails verwenden. Das Fenster enthält folgende Informationen und Möglichkeiten:

- Diagramm mit der Entwicklungskette der Bedrohung
- Empfehlungen zur Reaktion auf eine Bedrohung mit der Möglichkeit, die ausgewählte Aktion auszuführen
- Allgemeine Informationen zur Erkennung einer Bedrohung (z. B. den Modus der Erkennung)
- Informationen über das geschützte Gerät
- Informationen über das erkannte Objekt

- Verlauf des Auftretens von Dateien auf dem Gerät
- Informationen über die Aktionen, die von der Anwendung ergriffen wurden, um auf erkannte Bedrohung zu reagieren

Im Fenster mit den Alarmdetails können Sie die folgenden Reaktionsmaßnahmen ausführen:

- Das Gerät isolieren, auf dem die Bedrohung erkannt wurde.
- Die Datei in die Quarantäne verschieben.
- Eine Aufgabe zur *IOC-Untersuchung* erstellen.

Die Alarmdetails werden 30 Tage lang gespeichert. Nach dieser Zeit werden ältere Einträge automatisch gelöscht.

Weitere Informationen zum Arbeiten mit Alarmdetails finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum.

Integration von Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response ist eine Lösung, die basierend auf Telemetriedaten und fortschrittlichen Machine-Learning-Methoden etwaige Sicherheitsvorfälle in Ihrer Infrastruktur automatisch erkennt und analysiert. Die Informationen zu einem Vorfall werden an Kaspersky-Experten weitergeleitet, die den Vorfall anschließend selbst bearbeiten oder Empfehlungen zu dessen Lösung aussprechen.

Im Rahmen der Interaktion mit Kaspersky Managed Detection and Response kann Kaspersky Endpoint Security die folgenden Funktionen ausführen:

- Telemetriedaten zur Erkennung von Bedrohungen an Kaspersky Managed Detection and Response senden
- Ausführen von Reaktionsmaßnahmen, welche darauf abzielen, auf Grundlage von Befehlen, die von Kaspersky Managed Detection and Response empfangen wurden, die Schutzfunktionen zu gewährleisten.

Die Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response erfolgt über die Anwendungskomponente "Managed Detection and Response" (im Weiteren auch "MDR").

Um die Funktionen von Kaspersky Managed Detection and Response verwenden zu können, müssen Sie die MDR-Komponente auf eine der folgenden Arten aktivieren:

- Durch das Hinzufügen eines Lizenzschlüssels mithilfe einer Schlüsseldatei oder eines Aktivierungscodes. Sie können die Anwendung "Kaspersky Endpoint Security" mit einer Lizenz aktivieren, welche die Funktionen von Kaspersky Managed Detection and Response abdeckt (weitere Informationen finden Sie in der Hilfe zu Kaspersky Managed Detection and Response). Wenn von der Hauptlizenz, unter welcher Sie die Anwendung verwenden, die Funktionen von Kaspersky Managed Detection and Response nicht abgedeckt werden, müssen Sie für diese Funktionen eine separate Lizenz erwerben und deren MDR-Lizenzschlüssel zur Anwendung hinzufügen.

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

Eine Lizenz zur Aktivierung der Funktionen von Kaspersky Managed Detection and Response-Funktionalität erfordert die vorherige Registrierung im MDR-Portal.

- Indem Sie auf das Gerät eine *MDR-BLOB-Datei* hochladen, welche die Lizenzinformationen für Kaspersky Managed Detection and Response enthält. Die BLOB-Datei befindet sich im ZIP-Archiv der MDR-Konfigurationsdatei. Eine BLOB-Datei können Sie in der Web Console, in der Verwaltungskonsole oder über die Befehlszeile hochladen.

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.

Die Integration mit Kaspersky Managed Detection and Response besteht aus den folgenden Schritten:

1. **Aktivieren der erforderlichen Komponenten von Kaspersky Endpoint Security**

   Stellen Sie sicher, dass die folgenden Komponenten von Kaspersky Endpoint Security aktiviert sind und einsatzbereit sind:

   - Schutz vor bedrohlichen Dateien.
   - Verhaltensanalyse.

   Wenn diese Komponenten deaktiviert sind, hat das Gerät in Kaspersky Managed Detection and Response einen roten Status.

   Es wird außerdem empfohlen, die Komponenten Schutz vor Web-Bedrohungen und Schutz vor Netzwerkbedrohungen zu aktivieren. Wenn diese Komponenten deaktiviert sind, hat das Gerät in Kaspersky Managed Detection and Response einen gelben Status.

   Nähere Informationen zu den Statuswerten finden Sie in der Hilfe zu Kaspersky Managed Detection and Response.

2. **Aktivieren der Verwendung des erweiterten Modus von Kaspersky Security Network.**

   Die Funktionen von Kaspersky Managed Detection and Response sind nicht verfügbar, wenn Kaspersky Security Network deaktiviert ist oder im Standardmodus verwendet wird. Die Verwendung von Kaspersky Security Network können Sie in der Web Console, in der Verwaltungskonsole oder über die Befehlszeile konfigurieren.

3. **Aktivieren der MDR-Komponente**

Wenn Sie die MDR-Komponente unter einer Lizenz verwenden, stellen Sie sicher, dass eine der folgenden Bedingungen erfüllt ist:

- Sie verwenden die Anwendung "Kaspersky Endpoint Security" unter einer Lizenz, welche die Funktionalitäten von Managed Endpoint Detection and Response abdeckt.
- Sie haben eine separate Lizenz zur Nutzung der Funktionen von Kaspersky Managed Detection and Response erworben und einen zusätzlichen MDR-Lizenzschlüssel zur Anwendung hinzugefügt.

  Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, wird der Lizenzschlüssel zum Aktivieren zusätzlicher Funktionen auf der SVM hinzugefügt.

Wenn Sie die MDR-Komponente anhand einer MDR-BLOB-Datei aktivieren, müssen Sie die BLOB-Datei in der Web Console, in der Verwaltungskonsole oder über die Befehlszeile hochladen.

4. **Hochladen der KPSN-Konfigurationsdatei**

   Wenn Ihre Konfiguration nicht den Anforderungen für den Betrieb ohne KPSN-Konfigurationsdateien entspricht, müssen Sie die KPSN-Konfigurationsdatei auf den Administrationsserver von Kaspersky Security Center hochladen.

5. **Aktivieren der MDR-Komponente**

   Die MDR-Komponente ist standardmäßig deaktiviert. Aktivieren oder deaktivieren können Sie die Komponente:

   - Mittels Web Console
   - Mittels Verwaltungskonsole
   - Über die Befehlszeile

   Überprüfen können Sie den Ausführungsstatus der MDR-Komponente:

   - in den Geräteeigenschaften in der Web Console oder in der Verwaltungskonsole.
   - Über die Befehlszeile.

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.

KPSN-Konfigurationsdatei zur Integration von Kaspersky Managed Detection and Response hochladen

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 über die 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 die Verwaltungskonsole 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**.

Integration mit Kaspersky Managed Detection and Response in der Web Console konfigurieren

In der Web Console können Sie die Einstellungen zur Integration mit Kaspersky Managed Detection and Response in den Richtlinieneigenschaften konfigurieren (**Anwendungseinstellungen** → **Built-in Agents Configuration** → **Managed Detection and Response**).

Integration mit Kaspersky Managed Detection and Response in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie in den Richtlinieneigenschaften die MDR-Komponente aktivieren oder deaktivieren und eine MDR-BLOB-Datei laden (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Detection and Response** → **Managed Detection and Response**).

> Wenn Sie einen Lizenzschlüssel zum Aktivieren der MDR-Komponente verwenden, müssen Sie die MDR-BLOB-Datei nicht hochladen.

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.

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 mit Kaspersky Managed Detection and Response über die Befehlszeile konfigurieren

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.

- Ändern Sie die Startzeit der Dienstaufgabe *Mdr_Autostart_Scan*, die nach der Integration von Kaspersky Endpoint Security mit Managed Detection and Response automatisch erstellt wird.

Es wird empfohlen, die Konfiguration der Integration von Kaspersky Endpoint Security mit Kaspersky Managed Detection and Response in der Verwaltungskonsole oder in der Web Console durchzuführen.

Sie können die MDR-Komponente mithilfe des Parameters `UseMDR` in den allgemeinen Anwendungseinstellungen aktivieren oder deaktivieren. Sie können den Wert des Parameters mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen 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 <Dateipfad MDR-BLOB>
```

Führen Sie den folgenden Befehl aus, um die BLOB-Datei zu löschen:

```
Befehl kesl-control --remove-mdr-blob
```

Nach der Aktivierung der Integration wird in der Anwendung die Dienstaufgabe *Mdr_Autostart_Scan* erstellt und einmal am Tag ausgeführt. Bei Bedarf können Sie die Startzeit dieser Aufgabe konfigurieren. Andere Aufgabeneinstellungen und die Einstellungen der Aufgabenzeitpläne können nicht geändert werden.

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 Anwendung 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 von Kaspersky Endpoint Security mit der Lösung 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 einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection und mit Response (KATA) und Kaspersky Managed Detection and Response wird die Aktivierung und Deaktivierung der Netzwerkisolation des Geräts sowie die Konfiguration der Ausnahmen von der Netzwerkisolation in der entsprechenden Detection and Response-Lösung durchgeführt. Weitere Informationen dazu finden Sie in der Hilfe von Kaspersky Endpoint Detection and Response Expert (on-premise), in der Hilfe von Kaspersky Anti Targeted Attack Platform oder in der Hilfe von 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 im Fenster mit den Alarmdetails und in den Geräteeigenschaften in der Web Console manuell 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 Modus als Endpoint Detection and Response Agent verwendet wird und Netzwerkisolation aktiviert ist, wird Folgendes empfohlen:

- 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 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. 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.

     Wenn Sie auf diese Schaltfläche klicken, isoliert das Programm das Gerät für die in den Eigenschaften angegebene Dauer der Aufgabe *Netzwerkisolation aktivieren (NetworkIsolationStart)*.

   - Klicken Sie auf die Schaltfläche **Isoliertes Gerät freigeben**, um die Netzwerkisolierung des Geräts zu deaktivieren.

8. 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 Integration mit Kaspersky Endpoint Detection and Response Expert (lokal) 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 im Block **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 Alarmdetails aktiviert haben.

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 Eigenschaften der Aufgabe 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

Bei einer Integration von Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response wird die Netzwerkisolation in der entsprechenden Detection and Response-Lösung konfiguriert. Weitere Informationen dazu finden Sie in der Hilfe von Kaspersky Endpoint Detection and Response Expert (on-premise), in der Hilfe von Kaspersky Anti Targeted Attack Platform oder in der Hilfe von 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.

Ausnahmen von der Netzwerkisolation im automatischen Modus konfigurieren

Sie können die Ausnahmen von der Netzwerkisolation für Geräte, die automatisch isoliert werden, sowohl in den Richtlinieneigenschaften als auch in den Geräteeigenschaften konfigurieren. Die Parameter zur Netzwerkisolation in den Richtlinieneigenschaften der Web Console werden in Anhang 5 beschrieben.

Die Ausnahmen aus der Netzwerkisolation können nur bei einer Integration von Kaspersky Endpoint Detection and Response Optimum konfiguriert werden:

Das Hinzufügen oder Entfernen von Ausnahmen für die Netzwerkisolation ist in den Geräteeigenschaften nicht möglich, wenn das Gerät einer Richtlinie unterliegt.

So können Sie eine Ausnahme für die Netzwerkisolation hinzufügen oder entfernen:

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

   Die Liste der verwalteten Geräte wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die das erforderliche Gerät enthält. Klicken Sie dazu auf den Link im Feld **Aktueller Pfad** 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.

   Das Eigenschaftenfenster der App wird geöffnet.

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. Öffnen Sie im neuen Fenster im Parameterblock **Ausnahmen** durch Anklicken des Links **Ausnahmen konfigurieren** das Fenster **Ausnahmen**.

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**, um die Änderungen zu speichern.

Fenster "Ausnahme für die Netzwerkisolation hinzufügen"

In diesem Fenster können Sie Informationen über eine Netzwerkverbindung eingeben, die nach der Aktivierung der Netzwerkisolation nicht blockiert wird.

Einstellungen der Netzwerkverbindung

Parameter	Description
Name	Eingabefeld für den Namen der Netzwerkverbindung.
Richtung	In der Dropdown-Liste können Sie die Richtung der Netzwerkverbindung auswählen: • **Ausgehend** • **Eingehend** • **Eingehend/Ausgehend**

Parameter	Description
Protokoll	In der Dropdown-Liste können Sie das Protokoll für der Netzwerkverbindung auswählen: • **Alle** • **Benutzerdefiniert** • **ICMP** • **IPv6_ICMP**. • **TCP** • **UDP** • **IGMP** • **GRE** • **IPv4**. • **IPv6**
Nummer	Eingabefeld für den Namen der Netzwerkverbindung. Dieses Feld ist verfügbar, wenn in der Dropdown-Liste **Protokoll** die Option **Benutzerdefiniert** ausgewählt ist.
Lokale Ports/Portbereiche	Das Kontrollkästchen fügt die im Feld unten aufgeführten lokalen Portnummern oder lokalen Portbereiche zur Liste der Ausnahmen aus der Netzwerkisolation hinzu.
Remote-Ports/Portbereiche	Das Kontrollkästchen fügt die im Feld unten aufgeführten Remote-Portnummern oder Remote-Portbereiche zur Liste der Ausnahmen aus der Netzwerkisolation hinzu.
Remote-Adresse	Das Kontrollkästchen fügt die im Feld unten angegebene IP-Adresse des Remote-Geräts zur Liste der Ausnahmen aus der Netzwerkisolation hinzu.
Anwendungen	Das Kontrollkästchen fügt die in der Tabelle unter dem Kontrollkästchen aufgeführten Anwendungen zur Liste der Ausnahmen aus der Netzwerkisolation hinzu. Sie können den Pfad zu einer Anwendung hinzufügen, deren Netzwerkverbindung nicht blockiert werden soll, indem Sie auf die Schaltfläche **Hinzufügen** klicken. Geben Sie im nächsten Fenster im Feld **Pfad zur Anwendung** den Pfad zur Anwendung ein und speichern Sie die Änderungen. Sie können eine Anwendung aus der Tabelle entfernen, indem Sie das Kontrollkästchen neben der zu entfernenden Anwendung aktivieren und anschließend auf die Schaltfläche **Löschen** klicken. Diese Parameter gelten auf Geräten mit Kernel-Version 4.18 oder höher mit Unterstützung für eBPF mit BTF und mit aktivierten tracepoints-Funktionen und kprobes für das Kernel-Tracing.

Fenster "Liste mit Netzwerkprofilen"

In diesem Fenster können Sie ein oder mehrere Profile einer auszuschließenden Netzwerkverbindung auswählen.

Profile der Netzwerkverbindungen

Profil der Netzwerkverbindung	Description
DNS-Server	Dienst der die Auflösung von DNS-Namen ermöglicht, indem er auf Anfragen zum Abrufen von IP-Adressen und zum Aktualisieren von DNS-Einträgen reagiert.
DNS-Client	Dienst der die Auflösung von DNS-Namen ermöglicht, indem er Abfragen von DNS-Namen durchführt.
Active Directory-Zertifikatdienste (AD CS)	Dienste zum Erstellen, Validieren und Widerrufen öffentlicher Schlüsselzertifikate für die interne Verwendung innerhalb einer Organisation.
Active Directory-Verbunddienste (AD FS)	Dienste zum Ermöglichen des Benutzerzugriffs auf mehrere Webdienste oder Netzwerkressourcen mithilfe eines einzigen zentral gespeicherten Satzes von Anmeldeinformationen.
Active Directory Lightweight Directory Services (AD LDS)	Dienste, die eine Funktionalität wie die Domänendienste von Active Directory bereitstellen, jedoch ohne Notwendigkeit der Erstellung von Domänen oder Domänencontrollern.
Active Directory Rights Management Services (AD RMS)	Dienste zur Steuerung des Benutzerzugriffs auf Dokumente.
DHCP	Dienst, der das Dynamic Host Configuration Protocol (DHCP) verwendet, um IP-Adressen automatisch zuzuweisen.
File Transfer Protocol (FTP)	Standard-Netzwerkprotokoll, das zum Übertragen von Dateien zwischen Clients und einem Server in einem Netzwerk verwendet wird.

Profil der Netzwerkverbindung	Description
Kerberos-Schlüsselverteilungscenter	Netzwerkdienst, der zur Bereitstellung von Tickets (TGS) und temporären Sitzungsschlüsseln für Benutzer und Geräte in einer Active Directory-Domäne verwendet wird.
Secure Shell (SSH)	Ein Protokoll, das die Remote-Verwaltung des Betriebssystems und das Tunneln von TCP-Verbindungen ermöglicht.
Linux-Systemkomponenten	Linux-Systemdienste für Netzwerke wie NetworkManager.

Netzwerkisolation eines Geräts über die Befehlszeile verwalten

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*.

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 Parameter der Quarantäne auf dem Gerät über die Web Console, die Verwaltungskonsole und 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).

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.

Sie können systemkritische Objekte (SCO) nicht in die Quarantäne verschieben. SCOs umfassen Dateien, die für die Ausführung des Betriebssystems und von Kaspersky Endpoint Security erforderlich sind.

Das Verschieben einer Datei in die Quarantäne ist nur möglich, 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 von Kaspersky Endpoint Security mit der Lösung 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 Kaspersky Managed Detection and Response ist aktiviert und die MDR-Komponente ist aktiviert.

Für das Verzeichnis zum Speichern der Quarantäneobjekte sollte Schreibzugriff verfügbar sein.

Bei einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA) werden Dateien durch eine der folgenden Varianten in Quarantäne verschoben:

- Als Ausführungsergebnis einer Aufgabe, die in der jeweiligen Managed Detection and Response-Lösung konfiguriert ist. Weitere Informationen dazu 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 Ausführungsergebnis einer Aufgabe zur YARA-Untersuchung der Prozess-Speicher.

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.
- Als Ergebnis einer ausgeführten Empfehlung aus den Alarmdetails.

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.

Dateien mithilfe der Web Console in die Quarantäne verschieben

Bei Integration mit der Lösung "Kaspersky Endpoint Detection and Response Optimum" können Sie in der Web Console anhand der Aufgabe *Datei in Quarantäne verschieben* Dateien in die Quarantäne verschieben.

Sie können die Aufgabe "Datei in Quarantäne" verschieben sowohl für alle als auch für ausgewählte verwaltete Geräte erstellen und ausführen.

Die Aufgabe wird für die Dateien ausgeführt, die in den Aufgabeneingenschaften auf der Registerkarte **Anwendungseinstellungen** der in Tabelle **Datei in die Quarantäne verschieben** angegebenen sind. Die Tabelle enthält die folgenden Informationen zu Dateien, die in die Quarantäne verschoben werden sollen:

- **Pfad** – Pfad zu dem Verzeichnis auf dem Gerät, in dem sich die Datei befindet.
- **Typ der Prüfsumme** – Prüfmethode der Prüfsumme der Datei.

Mit den Schaltflächen oberhalb der Tabelle können Sie Informationen zu den Dateien, die in die Quarantäne verschoben werden sollen, hinzufügen oder löschen.

Um Informationen zu einer Datei, die in die Quarantäne verschoben werden soll, hinzuzufügen, müssen Sie auf die Schaltfläche **Hinzufügen** klicken und im neuen Fenster die Aufgabenparameter angeben.

Einstellungen der Aufgabe "Datei in die Quarantäne verschieben"

Parameter	Description
Geben Sie die Datei an, die in die Quarantäne verschoben werden soll	In der Dropdown-Liste können Sie die Methode zur Pfadangabe zu der Datei auswählen, die in die Quarantäne verschoben werden soll: • **Datei mittels vollständigen Pfad angeben**. • **Datei mittels Verzeichnispfad und Prüfsumme angeben**.
Vollständiger Pfad zur Datei	Eingabefeld für den vollständigen Pfad der Datei, die in die Quarantäne verschoben werden soll. Dieses Feld wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die Datei an, die in die Quarantäne verschoben werden soll** den Wert **Datei mittels vollständigen Pfad angeben** ausgewählt haben. Wenn sich die Datei auf einem Netzlaufwerk befindet, geben Sie am Anfang des Dateipfads die Zeichen `//` ein. Sie können beispielsweise den Pfad `//server_ip/shared_folder` eingeben.
Typ der Prüfsumme	In der Dropdown-Liste können Sie den Typ der Prüfsumme für die Datei auswählen, die in die Quarantäne verschoben werden soll: • **MD5**. • **SHA256** Diese Dropdown-Liste wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die Datei an, die in die Quarantäne verschoben werden soll** den Wert **Datei mittels Verzeichnispfad und Prüfsumme angeben** ausgewählt haben.
Prüfsumme der Datei	Eingabefeld für die Prüfsumme der Datei, die in die Quarantäne verschoben werden soll. Dieses Feld wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die Datei an, die in die Quarantäne verschoben werden soll** den Wert **Datei mittels Verzeichnispfad und Prüfsumme angeben** ausgewählt haben.

Parameter	Description
Dateipfad	Eingabefeld für den Pfad zum Verzeichnis der Datei, die in die Quarantäne verschoben werden soll. Dieses Feld wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die Datei an, die in die Quarantäne verschoben werden soll** den Wert **Datei mittels Verzeichnispfad und Prüfsumme angeben** ausgewählt haben. Wenn sich die Datei auf einem Netzlaufwerk befindet, geben Sie am Anfang des Dateipfads die Zeichen `//` ein. Sie können beispielsweise den Pfad `//server_ip/shared_folder` eingeben.

Die Aufgabe *Datei in die Quarantäne verschieben* schlägt möglicherweise mit der Fehlermeldung *Unzureichender Speicherplatz im Quarantäne-Speicher* fehl, wenn Sie versuchen, eine große Datei in die Quarantäne zu verschieben. In diesem Fall müssen Sie die Quarantäne leeren oder deren Größe erhöhen und es anschließend erneut versuchen.

Nach der Ausführung der Aufgabe können Sie deren Ergebnis in den Eigenschaften der Web Console im Abschnitt **Ergebnisse** anzeigen.

Quarantäne-Einstellungen in Web Console konfigurieren

In der Web Console können Sie Quarantäne-Einstellungen in den Richtlinieneigenschaften (**Programmeinstellungen** → **Allgemeine Einstellungen** → **Berichte und Speicher**) und in den Eigenschaften verwalteter Geräte (**Assets (Geräte)** → **Verwaltete Geräte** → Link <Gerätename> → Registerkarte **Anwendungen** → Link <Name des Kaspersky Endpoint Security-Programms> → Registerkarte **Programmeinstellungen** → Abschnitt **Speichereinstellungen**) verwalten.

Die Quarantäne-Einstellungen in den Eigenschaften des verwalteten Geräts werden in der folgenden Tabelle beschrieben.

Parameter der Quarantäne in den Geräteeigenschaften

Parameter	Description
Größe der Quarantäne begrenzen auf (MB)	Eingabefeld zur Angabe der maximalen Quarantäne-Größe (in Megabyte). Wenn kein Häkchen gesetzt wurde, ist die Größe der Quarantäne unbegrenzt. Standardwert: 200.
Benachrichtigen, wenn Quarantäne gefüllt ist zu (%)	Eingabefeld zur Angabe des Prozentsatzes der Quarantäne-Füllstands, bei dessen Erreichen ein Ereignis über die Auslastung der Quarantäne gesendet wird. Wenn das Kontrollkästchen deaktiviert ist, werden keine Ereignisse zum Quarantäne-Füllstand generiert. Zulässige Werte: 1 – 100. Standardwert: 90

Quarantäne-Einstellungen in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie Quarantäne-Einstellungen in den Richtlinieneigenschaften (Verwalten von Richtlinien in der Verwaltungskonsole, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Allgemeine Einstellungen** → **Speichereinstellungen**) und in den Eigenschaften verwalteter Geräte (**Verwaltete Geräte** → Registerkarte **Geräte** → Fenster mit den Geräteeigenschaften → Abschnitt **Anwendungen** → Fenster mit den Programmeigenschaften → **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 beträgt 200, wenn die Anwendung im Standard-Modus oder im Modus als Endpoint Detection and Response Agent verwendet wird, und 100, wenn die Anwendung 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

Quarantäne-Einstellungen über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Quarantäne-Einstellungen mithilfe der Optionen `QuarantineSizeLimit`, `QuarantineFillingNotification` und `QuarantineBackupFolder` in den allgemeinen Anwendungseinstellungen konfigurieren.

Sie können den Wert von Parametern mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen 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 – 999999 0 – Die Größe der Quarantäne ist nicht begrenzt. Der Standardwert beträgt 200, wenn die Anwendung im Standard-Modus oder im Modus als Endpoint Detection and Response Agent verwendet wird, und 100, wenn die Anwendung 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 <Dateipfad> [--md5] [--sha256] [--save-original-file]
```

wobei:

- `<Dateipfad>` – Pfad 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 ["<Filterbedingungen>"] [-n <Anzahl>] [--json]
```

wobei:

- Mit `<Filterbedingungen>` werden ein oder mehrere logische Ausdrücke im Format `<Feld> <Vergleichsoperation> '<Wert>'` angegeben, die mit dem logischen Operator `and` kombiniert werden, um Abfrageergebnisse einzuschränken. Wenn Sie keine Filterbedingungen angeben, zeigt die Anwendung Informationen zu allen Quarantäne-Dateien an.
- `<Zahl>` 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 <Objekt-ID>
```

Dabei steht `<Objekt-ID>` für eine numerische ID, die das Programm 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 <Objekt-ID> --file <Dateipfad>
```

Dabei steht `--file <Dateipfad>` 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.

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 "<Filterbedingungen>"
```

Dabei steht `<Filterbedingungen>` für einen oder mehrere logische Ausdrücke im Format `<Feld> <Vergleichsoperator> '<Wert>'`, die mithilfe des logischen Operators `and` kombiniert werden, um die Ergebnisse einzuschränken.

Beispiele:
So löschen Sie 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
```

Einen Prozess starten

Bei einer Integration von Kaspersky Endpoint Security mit Detection and Response-Lösungen, können Sie mithilfe der Aufgabe zum Starten eines Prozesses (*Run process*) die Prozesse und ausführbaren Dateien auf einem geschützten Gerät remote starten.

Nur bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie Aufgaben zum Starten eines Prozesses in der Web Console erstellen und ausführen. Bei einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response werden die Aufgaben von der entsprechenden Detection and Response-Lösung erstellt und ausgeführt.

Anhand der Aufgabe *Prozess starten* können Sie Folgendes starten:

- Prozesse, die aufgrund böswilliger Aktivitäten auf dem Gerät beendet wurden.
- Prozesse, die Sie beendet haben. Sie können beispielsweise einen Prozess, den Sie mit der Aufgabe *Prozess beenden* beendet haben, aus remote starten.
- Skripte. Sie können beispielsweise ein Skript ausführen, um Daten von einem Gerät zu sammeln, die zur Untersuchung einer Bedrohung gedacht sind.

- Tools. Sie können beispielsweise ein Tool ausführen, das die Informationen zu einer Gerätekonfiguration in einer Datei speichert.
- Anwendungen.

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

Sie können in der Web Console die Aufgabe *Prozess starten* erstellen und ausführen sowie ihre Einstellungen bearbeiten: Die Aufgabe *Prozess starten* kann nicht über die Befehlszeile verwaltet werden.

Parameter der Aufgabe zum Starten eines Prozesses

Parameter	Description
Ausgeführter Befehl	Eingabefeld für den Startbefehl des Prozesses. Wenn Sie beispielsweise das Tool `klnagchk` ausführen möchten, mit dem die Verbindung zum Administrationsserver überprüft werden soll, müssen Sie `/< absoluter Pfad zum Verzeichnis des Tools >/klnagchk` eingeben und anschließend bei Bedarf die übrigen in der unteren Tabelle beschriebenen Felder ausfüllen.
Befehlszeilenargumente (optional)	Eingabefeld für Befehlszeilenargumente zur Übergabe zusätzlicher Informationen an das Skript, das Tool oder die Anwendung beim Start. Sie können beispielsweise das Argument `-logfile /tmp/klnagchk.log` eingeben. Dieses Argument weist das Tool an, das Ergebnis in einer Datei namens `klnagchk.log` im Verzeichnis `/tmp` zu speichern. Wenn Sie mehrere Argumente übergeben möchten, müssen Sie diese durch ein Leerzeichen trennen. Sie können beispielsweise die Argumente `-logfile /tmp/klnagchk.log -savecert /home/user/certificate.cer` eingeben. Diese Argumente weisen das Tool an, das Ergebnis in einer Datei namens `klnagchk.log` im Verzeichnis `tmp` zu speichern und das Zertifikat, das zur Überprüfung des Zugriffs auf den Administrationsserver verwendet wird, in der Datei `certificate.cer` im Verzeichnis `/home/user/` zu speichern.
Pfad zum Arbeitsverzeichnis (optional)	Feld für den Pfad zum Arbeitsverzeichnis, in dem der Befehl aus dem Feld **Ausführbarer Befehl** ausgeführt wird. Sie können beispielsweise `/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.

Nach der Ausführung der Aufgabe *Prozess starten* können Sie deren Ergebnis in den Eigenschaften der Web Console im Abschnitt **Anwendungseinstellungen** → **Ausführungsergebnisse** anzeigen.

Die Tabelle enthält eine Liste der Geräte, auf denen die Aufgabe *Prozess starten* ausgeführt wurde, sowie die Ergebnisse der Aufgabe. In der Dropdown-Liste **Gerät** können Sie auswählen, ob Ergebnisanzeige der Aufgabe für alle verwalteten Geräte, auf denen die Aufgabe gestartet wurde, oder für ein bestimmtes Gerät angezeigt werden soll.

Die Tabelle enthält die folgenden Informationen:

- **Status** – Status der Aufgabenausführung
- **Gerät** – Name des Geräts, auf dem die Aufgabe gestartet wurde.
- **Zeitpunkt** – Datum und Uhrzeit der Ausführung der Aufgabe.
- **Ergebnisse** – Ergebnis der Aufgabenausführung in Form eines Rückgabecodes. Der Link mit dem Rückgabecode öffnet das Fenster **Aufgabenergebnisse**, in dem die folgenden Informationen angezeigt werden:
  - Status der Aufgabenausführung
  - Startzeitpunkt des Prozesses

- Endzeitpunkt des Prozesses
- Name des Geräts, auf dem der Prozess gestartet wurde
- ausgeführter Befehl
- Befehlszeilenargumente
- Pfad zum Arbeitsverzeichnis
- Rückgabe-Code

Über den Link **STDOUT-Streamdaten herunterladen** im Fenster **Ergebnisse des Aufgabenstarts** können Sie einen Bericht über die erfolgreiche Aufgabenausführung im txt-Format herunterladen. Wenn die Aufgabe *Prozess starten* mit einem Fehler beendet wurde, wird beim Versuch, den Bericht herunterzuladen, eine Fehlermeldung angezeigt.

Über den Link **STDERR-Streamdaten herunterladen** im Fenster **Ergebnisse des Aufgabenstarts** können Sie einen Bericht über Fehler, die während der Aufgabenausführung aufgetreten sind, im txt-Format herunterladen. Wenn die Aufgabe *Prozess starten* erfolgreich beendet wurde, wird beim Versuch, den Bericht herunterzuladen, eine Fehlermeldung angezeigt.

Eines Prozesses beenden

Bei einer Integration von Kaspersky Endpoint Security mit Detection and Response-Lösungen, können Sie mithilfe der Aufgabe zum Beenden eines Prozesses (*Terminate process*) die Prozesse auf einem geschützten Gerät remote beenden.

Nur bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie Aufgaben zum Beenden eines Prozesses in der Web Console erstellen und ausführen. Bei einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response werden die Aufgaben von der entsprechenden Detection and Response-Lösung erstellt und ausgeführt.

Anhand der Aufgabe *Prozess beenden* können Sie Folgendes beenden:

- Prozesse, die aufgrund böswilliger Aktivitäten auf dem Gerät gestartet wurden.
- Prozesse, die Sie gestartet haben. Sie können beispielsweise einen Prozess, den Sie mit der Aufgabe *Prozess starten* gestartet haben, per Fernzugriff beenden.
- Skripte. Sie können beispielsweise ein Skript, das Sie mit der Aufgabe *Prozess starten* gestartet haben, per Fernzugriff beenden.
- Tools. Sie können beispielsweise ein Tool zur Messung der Internetgeschwindigkeit, das Sie mit der Aufgabe *Prozess starten* gestartet haben, per Fernzugriff beenden.
- Anwendungen.

Die Prozesse von systemkritischen Objekten (SCOs) können nicht beendet werden. SCOs umfassen Dateien, die für die Ausführung des Betriebssystems und von Kaspersky Endpoint Security erforderlich sind.

Sie können in der Web Console die Aufgabe *Prozess beenden* erstellen und ausführen sowie ihre Einstellungen bearbeiten: Die Aufgabe *Prozess beenden* kann nicht über die Befehlszeile verwaltet werden.

Parameter der Aufgabe zum Beenden eines Prozesses

Parameter	Description
Geben Sie die Datei an, deren Prozesse beendet werden soll	In der Dropdown-Liste können Sie die Methode zur Pfadangabe auswählen: • **Nach Pfad zum Verzeichnis und Prüfsumme**. • **Nach vollständigem Pfad** • **Nach PID** Der Wert **Nach PID** wird in der Dropdown-Liste nur für Aufgaben angezeigt, die in den Geräteeigenschaften erstellt wurden.
Vollständiger Pfad zur Datei	Eingabefeld für den vollständigen Pfad zur Datei. Dieses Feld wird nur angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die Datei an, deren Prozesse beendet werden soll** die Option **Nach vollständigem Pfad** ausgewählt haben.
Typ der Prüfsumme	In der Dropdown-Liste können Sie die zu verwendende Prüfsumme der Datei auswählen: • **MD5**. • **SHA256** Diese Dropdown-Liste wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die Datei an, deren Prozesse beendet werden sollen** die Option **Nach Pfad zum Verzeichnis und Prüfsumme** auswählen.
Prüfsumme der Datei	Eingabefeld für die Prüfsumme der Datei Dieses Feld wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die Datei an, deren Prozesse beendet werden soll** die Option **Nach Pfad zum Verzeichnis und Prüfsumme** und in der Dropdown-Liste **Typ der Prüfsumme** den Wert **MD5** angegeben haben.
Pfad zum Verzeichnis	Eingabefeld für Pfad zum Dateiverzeichnis. Dieses Feld wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die Datei an, deren Prozesse beendet werden soll** die Option **Nach Pfad zum Verzeichnis und Prüfsumme** ausgewählt haben.
Prozess-ID	Eingabefeld für die Prozess-ID (PID) Dieses Feld wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die Datei an, deren Prozesse beendet werden soll** die Option **Nach PID** ausgewählt haben.

Nach der Ausführung der Aufgabe *Prozess beenden* können Sie deren Ergebnis in den Eigenschaften der Web Console im Abschnitt **Ergebnisse** anzeigen.

Datei von Gerät abrufen

Bei einer Integration von Kaspersky Endpoint Security mit Detection and Response-Lösungen, können Sie anhand der Aufgabe zum Abrufen von Dateien (*Get file*) Dateien von einem geschützten Gerät abrufen.

Nur bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie Aufgaben zum Abrufen einer Datei von einem Gerät in der Web Console erstellen und ausführen. Bei einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise), mit Kaspersky Endpoint Detection and Response (KATA) oder mit Kaspersky Managed Detection and Response werden die Aufgaben von der entsprechenden Detection and Response-Lösung erstellt und ausgeführt.

Beispielsweise können Sie eine Ereignisprotokoll-Datei abrufen, die von der Anwendung eines Drittanbieters generiert wurde.

Sie können in der Web Console die Aufgabe *Empfangen einer Datei von einem Gerät* erstellen und ausführen sowie ihre Einstellungen bearbeiten: Die Aufgabe *Datei vom Gerät empfangen* kann nicht über die Befehlszeile verwaltet werden.

Die Aufgabe *Datei von Gerät abrufen* wird für die Dateien ausgeführt, die in den Aufgabeneingenschaften auf der Registerkarte **Anwendungseinstellungen** der in Tabelle **Datei abrufen** angegebenen sind.

Die Tabelle enthält die folgenden Informationen zu den Dateien, die durch die Aufgabe abgerufen werden sollen:

- **Pfad zum Verzeichnis** – Pfad zu dem Verzeichnis auf dem Gerät, in dem sich die Datei befindet.
- **Prüfmethode der Prüfsumme** – Prüfmethode der Prüfsumme der Datei.

Mit den Schaltflächen oberhalb der Tabelle können Sie Informationen zu den Dateien, die vom Gerät abgerufen werden sollen, hinzufügen, ändern oder löschen.

Um Informationen zu einer Datei, die abgerufen werden soll, hinzuzufügen, müssen Sie auf die Schaltfläche **Hinzufügen** klicken und im neuen Fenster **Datei abrufen** die Aufgabenparameter angeben.

Parameter der Aufgabe zum Abrufen einer Datei von einem Gerät

Parameter	Description
Geben Sie die abzurufende Datei an	In der Dropdown-Liste können Sie die Methode zur Pfadangabe auswählen: • **Nach Pfad zum Verzeichnis und Prüfsumme**. • **Nach vollständigem Pfad**
Vollständiger Pfad zur Datei	Eingabefeld für den vollständigen Pfad zur Datei. Dieses Feld wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die abzurufende Datei an** die Option **Nach vollständigem Pfad** ausgewählt haben.
Typ der Prüfsumme	In der Dropdown-Liste können Sie die zu verwendende Prüfsumme der Datei auswählen: • **MD5**. • **SHA256** Diese Dropdown-Liste wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die abzurufende Datei an** die Option **Nach Pfad zum Verzeichnis und Prüfsumme** auswählen.
Prüfsumme der Datei	Eingabefeld für die Prüfsumme der Datei Dieses Feld wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die abzurufende Datei an** die Option **Nach Pfad zum Verzeichnis und Prüfsumme** ausgewählt haben.
Pfad zum Verzeichnis der Datei	Eingabefeld für Pfad zum Dateiverzeichnis. Dieses Feld wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die abzurufende Datei an** die Option **Nach Pfad zum Verzeichnis und Prüfsumme** ausgewählt haben.

Als Ergebnis der Ausführung der Aufgabe *Datei von Gerät abrufen* wird eine Kopie der Datei in der Quarantäne des Geräts gespeichert. Über die Web Console können Sie diese Kopie aus der Quarantäne auf das Gerät herunterladen, von dem Sie den Download initiiert haben.

Die Datei darf maximal 100 MB groß sein.

Die Originaldatei auf dem Gerät des Benutzers verbleibt im Originalverzeichnis.

In Kaspersky Security Center in der Liste der Dateien, die in Quarantäne verschoben wurden, haben alle Dateien, die mittels der Aufgabe *Datei von Gerät abrufen* empfangen wurden, den Status *Infiziert*, unabhängig von ihren Untersuchungsergebnissen.

Die Aufgabe *Datei vom Gerät abrufen* wird in den folgenden Fällen mit einem Fehler abgeschlossen:

- 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).

Nach der Ausführung der Aufgabe können Sie deren Ergebnis in den Eigenschaften der Web Console im Abschnitt **Ergebnisse** anzeigen.

Datei von Gerät löschen

Bei einer Integration von Kaspersky Endpoint Security mit Detection and Response-Lösungen, können Sie anhand der Aufgabe zum Löschen von Dateien (*Delete file*) Dateien von einem geschützten Gerät löschen.

Nur bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie Aufgaben zum Löschen einer Datei in der Web Console erstellen und ausführen. Bei einer Integration mit Kaspersky Endpoint Detection and Response (KATA) wird die Aufgabe in Kaspersky Endpoint Detection and Response (KATA) erstellt und gestartet.

Systemkritische Objekte (SCO) können nicht gelöscht werden. SCOs umfassen Dateien, die für die Ausführung des Betriebssystems und von Kaspersky Endpoint Security erforderlich sind.

Sie können in der Web Console die Aufgabe *Datei vom Gerät löschen* erstellen und ausführen sowie ihre Einstellungen bearbeiten: Die Aufgabe *Datei vom Gerät löschen* kann nicht über die Befehlszeile verwaltet werden.

Parameter der Aufgabe zum Löschen einer Datei von einem Gerät

Parameter	Description
Geben Sie die zu löschende Datei an	In der Dropdown-Liste können Sie die Methode für die Pfadangabe zur zu löschenden Datei auswählen: • **Nach Pfad und Prüfsumme**. • **Nach vollständigem Pfad**
Vollständiger Pfad zur Datei	Eingabefeld für den vollständigen Pfad zur zu löschenden Datei. Dieses Feld wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die zu löschende Datei an** die Option **Nach vollständigem Pfad** ausgewählt haben.
Typ der Prüfsumme	In der Dropdown-Liste können Sie die zu verwendende Prüfsumme der zu löschenden Datei auswählen: • **MD5**. • **SHA256** Diese Dropdown-Liste wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die zu löschende Datei an** die Option **Nach Pfad zum Verzeichnis und Prüfsumme** ausgewählt haben.
Prüfsumme der Datei	Eingabefeld für die Prüfsumme der zu löschenden Datei. Dieses Feld wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die zu löschende Datei an** die Option **Nach Pfad und Prüfsumme** ausgewählt haben.

Parameter	Description
Pfad zum Verzeichnis	Eingabefeld für Pfad zum Verzeichnis der zu löschenden Datei. Dieses Feld wird angezeigt, wenn Sie in der Dropdown-Liste **Geben Sie die zu löschende Datei an** die Option **Nach Pfad und Prüfsumme** ausgewählt haben.
Unterverzeichnisse einschließen	Dieses Kontrollkästchen schließt Unterverzeichnisse ein oder aus.

Wenn die Datei durch einem anderen Prozess gesperrt wird, wird die Aufgabe mit dem Status *Abgeschlossen* angezeigt, die Datei selbst wird jedoch erst nach einem Neustart des Geräts gelöscht. Stellen Sie nach einem Neustart des Geräts sicher, dass die Datei gelöscht wurde.

Die Aufgabe *Datei vom Gerät löschen* kann mit dem Fehler *Zugriff verweigert* abschließend, wenn Sie versuchen, eine laufende ausführbare Datei zu löschen. In diesem Fall müssen Sie die Aufgabe *Prozess beenden* für die Datei erstellen und ausführen und es anschließend erneut versuchen.

Nach der Ausführung der Aufgabe können Sie deren Ergebnis in den Eigenschaften der Web Console im Abschnitt **Ergebnisse** anzeigen.

IOC-Untersuchung

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. Bei einer Integration von Kaspersky Endpoint Security mit Detection and Response-Lösungen können Sie auf geschützten Geräten Kompromittierungsindikatoren erkennen und Maßnahmen ergreifen, um auf Bedrohungen zu reagieren durchzuführen.

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.
- Die Integration von Kaspersky Endpoint Security mit der Lösung 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.

Bei einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA) wird die IOC-Untersuchung in der entsprechenden Lösung ausgeführt.

Bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum wird die IOC-Untersuchung mithilfe der Aufgabe zur IOC-Untersuchung durchgeführt (*IOC Scan*). Sie können die Aufgabe zur IOC-Untersuchung erstellen:

- in der Web Console
- im Fenster mit den Alarmdetails
- Über die Befehlszeile

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 vorbereitet wurden. 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.

Über die Web Console nach Kompromittierungsindikatoren suchen

Nur bei einer Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie Suche nach Kompromittierungsindikatoren anhand der IOC-Untersuchungsaufgabe in der Web Console ausführen. Bei einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA) wird die IOC-Untersuchung in der entsprechenden Detection and Response-Lösung ausgeführt.

Sie können die Aufgabe IoC-Untersuchung in der Web Console erstellen, *ausführen* und deren Parameter ändern.

Für die Aufgabe *IOC-Untersuchung* ist in den Einstellungen des Zeitplans die Option für Wake-on-LAN nicht verfügbar. Um die Aufgabe auszuführen, stellen Sie sicher, dass das Gerät eingeschaltet ist.

Sie können die Haupteinstellungen der Aufgabe *IOC-Untersuchung* in den Aufgabeneigenschaften auf der Registerkarte **App-Einstellungen** → **Einstellungen für die IOC-Untersuchung** ändern.

Einstellungen der Aufgabe *IOC-Untersuchung*

Parameter	Description
IOC-Dateien neu definieren	Über diese Schaltfläche wird der Bereich **IOC-Dateien neu definieren** geöffnet. Die im Bereich **IOC-Dateien neu definieren** befindliche Schaltfläche **IOC-Dateien hinzufügen** öffnet ein Fenster, in dem Sie die für die Suche nach Kompromittierungsindikatoren erforderlich IOC-Dateien auf dem Gerät auswählen und herunterladen können. Nach dem Herunterladen der IOC-Dateien können Sie die Liste der Indikatoren aus den IOC-Dateien anzeigen.
IOC-Sammlung exportieren	Über diese Schaltfläche werden die IOC-Dateien auf das Gerät heruntergeladen.

Parameter	Description
Bei Erkennung eines IOCs folgende Reaktion anwenden	Das Kontrollkästchen aktiviert oder deaktiviert die Anwendung von Antwort-Reaktionen auf erkannte Anzeichen einer Gefährdung. Wenn das Kontrollkästchen aktiviert ist und Anzeichen einer Gefährdung erkannt werden, führt die Anwendung die von Ihnen ausgewählten Reaktionen aus: • **Untersuchung wichtiger Bereiche starten**. Wenn das Kontrollkästchen aktiviert ist und Anzeichen einer Gefährdung erkannt werden, führt startet die Anwendung die Aufgabe *Untersuchung wichtiger Bereiche*. Standardmäßig überprüft Kaspersky Endpoint Security den Kernel-Speicher, die gestarteten Prozesse, die Bootsektoren und andere **kritische Objekte**. ◦ /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 das Kontrollkästchen aktiviert ist und Kompromittierungsindikatoren erkannt werden, speichert die Anwendung eine Kopie des Objekts in der Quarantäne und löscht das Originalobjekt.

Parameter	Description
	• **Gerät vom Netzwerk isolieren**. Wenn dieses Kontrollkästchen aktiviert ist und Anzeichen einer Gefährdung erkannt werden, isoliert die Anwendung das Gerät vom Netzwerk, um eine Ausbreitung der Bedrohung zu verhindern. Sie können die Dauer der Isolation anpassen. Wenn das isolierte Gerät von einer Richtlinie abgedeckt wird, werden sowohl die Parameter für das automatische Ausschalten der Isolierung nach einem bestimmten Zeitraum als auch die in den Richtlinieneigenschaften angegebenen Parameter für die Ausschlüsse aus der Netzwerkisolation angewendet. Wenn das isolierte Gerät nicht von der Richtlinie abgedeckt ist, werden die in den Geräteeigenschaften angegebenen Parameter angewendet. Wenn das Kontrollkästchen deaktiviert ist, führt die App beim Erkennen von Anzeichen einer Gefährdung keine Aktionen zur Reaktion auf Bedrohungen aus. Informationen zur Erkennung von Kompromittierungsindikatoren werden sowohl im Fenster mit den Alarmdetails als auch in den Aufgabeneigenschaften angezeigt.

Sie können weitere Parameter der Aufgabe *IOC-Untersuchung* in den Eigenschaften der Aufgabe auf der Registerkarte **Anwendungseinstellungen** → **Erweitert** ändern.

Die Einstellungen im Abschnitt **Erweitert** können geändert werden, wenn Sie im Bereich **IOC-Dateien neu definieren** eine IOC-Datei hochgeladen haben.

Erweiterte Einstellungen der Aufgabe *IOC-Untersuchung*

Parameter	Description
Datentypen (IOC-Dokumente), die während der IOC-Untersuchung analysiert werden sollen	Die Kontrollkästchen im Abschnitt **Erweitert** fügen die folgenden Datentypen (IOC-Dokumente) zur Analyse während einer IOC-Untersuchung hinzu: • **Prozesse - ProcessItem** • **Dateien - FileItem** • **IOC-Dokumente** Der Link **IOC-Dokumente** ist verfügbar, wenn Sie im Bereich **IOC-Dateien neu definieren** eine IOC-Datei hochgeladen haben. Über diesen Link gelangen Sie zum Fenster **Parameter für die Dateiuntersuchung – FileItem**, in welchem Sie Untersuchungsbereiche hinzufügen können. • **ARP-Tabellen - ArpEntryItem** • **Netzwerkports - PortItem** • **Benutzerkonten - UserItem** • **Systemobjekte - SystemItem**
IOCs in den folgenden Bereichen suchen:	Das Kontrollkästchen aktiviert oder deaktiviert die Untersuchung der folgenden Bereiche: • **Dateien auf allen Laufwerken des Geräts** • **Dateien auf dem Systemlaufwerk des Geräts**. • **Kritische Bereiche des Geräts** Diese Option ist standardmäßig ausgewählt. • **Vordefinierte Bereiche nicht untersuchen**.
Angegebene Bereiche untersuchen	Das Kontrollkästchen fügt die Bereiche zur Liste der Untersuchungsbereiche hinzu, die in der Tabelle unterhalb des Kontrollkästchens aufgeführten werden. Über die Schaltfläche **Hinzufügen** können Sie zusätzliche Pfade zu Bereichen hinzufügen, die überprüft werden sollen. Geben Sie im nächsten Fenster im Feld **Bereich** den Pfad zum gewünschten Bereich an und speichern Sie die Änderungen. Sie können einen Bereich aus der Tabelle entfernen, indem Sie das Kontrollkästchen neben dem zu löschenden Bereich aktivieren und anschließend auf die Schaltfläche **Löschen** klicken. Sie können das Kontrollkästchen nicht deaktivieren, wenn in der Liste **IOCs in den folgenden Bereichen suchen** die Option **Vordefinierte Bereiche nicht untersuchen** ausgewählt ist.

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, neue Aufgaben zu erstellen.

Nach der Ausführung der Aufgabe *IOC-Untersuchung* können Sie deren Ergebnis in den Eigenschaften der Web Console im Abschnitt **Anwendungseinstellungen → Ergebnisse der IOC-Untersuchung** anzeigen. Die Tabelle enthält eine Liste der Geräte, auf denen die Aufgabe zur *IOC-Untersuchung* ausgeführt wurde, sowie die Ergebnisse der Aufgabe. In der Dropdown-Liste **Gerät** können Sie auswählen, ob Ergebnisanzeige der Aufgabe für alle verwalteten Geräte, auf denen die Aufgabe gestartet wurde, oder für ein bestimmtes Gerät angezeigt werden soll.

Die Tabelle enthält die folgenden Informationen:

- **Status** – Als Symbol angezeigter Erkennungsstatus der Kompromittierungsindikatoren.
- **Gerät** – Name des Geräts, auf dem die Aufgabe gestartet wurde.
- **Zeitpunkt** – Datum und Uhrzeit der Ausführung der Aufgabe.
- **Ergebnisse** – Informationen zum Ausführungsergebnis der *IoC-Untersuchungsaufgabe*. Es kann einer der folgenden Statuswerte angezeigt werden:
  - *IOC erkannt* – Dieser Status wird als Link angezeigt, der beim Anklicken ein Fenster mit den Alarmdetails öffnet.
  - *Keine IOCs erkannt*.

Die Aufbewahrungsdauer der Ergebnisse der IOC-Untersuchung beträgt 30 Tage. Danach beginnt Kaspersky Endpoint Security automatisch mit der Löschung alter Einträge.

Über die Befehlszeile nach Kompromittierungsindikatoren suchen

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 einer Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit Kaspersky Endpoint Detection and Response (KATA) wird die IOC-Untersuchung in 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 <Pfad zu Verzeichnis oder Datei> [--process
on|off] [--hint <regulärer Ausdruck>] [--arpentry on|off] [--ports on|off] [--system
on|off] [--files on|off] [--drives all|system|critical|custom] [--excludes <Liste der
Ausschlüsse>] [--scope <Liste der Verzeichnisse>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

wobei:

- `--path <Pfad zum Verzeichnis oder zur Datei>` 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 <regulärer Ausdruck>` 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 <Liste der Ausnahmen>` ist die Liste der Pfade, die von Untersuchungen ausgeschlossen sind.

  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 <Liste der Verzeichnisse>` 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 der **kritischen Bereiche** durch.
    - /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.

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`
	◦ Unter Verwendung des Operators `TO` im Feld `Content`
	Die Anwendung unterstützt die Interpretation der Datentypen `date` und `duration`, wenn die Indikatoren im Format `ISO 8601, Zulu time zone, UTC` angegeben sind.

Ausführungsprävention für Objekte

Bei einer Integration mit Detection and Response-Lösungen kann Kaspersky Endpoint Security im Rahmen einer Maßnahme zur Reaktion auf eine Bedrohung den Start ausführbarer Dateien und Skripte sowie das Öffnen von Office-Dateien auf dem Gerät überwachen. 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 erfolgt auf Grundlage der Regeln der Ausführungsprävention. Eine *Regel der Ausführungsprävention* besteht aus einer Reihe von Kriterien, die Kaspersky Endpoint Security bei der Reaktion auf einen gestarteten Prozess berücksichtigt. Ein Objekt muss alle Kriterien einer Regel zur Ausführungsprävention erfüllen, damit die Anwendung den Start des Objekts blockiert. Die Anwendung identifiziert Dateien anhand von Pfaden oder Prüfsummen, die auf MD5- und SHA256-Hash-Algorithmen beruhen.

Die Ausführungsprävention für Objekte 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.
- Die Integration von Kaspersky Endpoint Security mit der Lösung 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.

Wenn sich der Interceptor für Dateioperationen nicht im Blockiermodus befindet, wird die Ausführungsprävention von Objekten unabhängig vom festgelegten Modus im Benachrichtigungs-Modus ausgeführt.

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.

Besonderheiten der Ausführungsprävention bei Integration mit Kaspersky Endpoint Detection and Response Expert (lokal) oder Kaspersky Endpoint Detection and Response (KATA)

Bei der Integration von Kaspersky Endpoint Security mit der Lösung Kaspersky Endpoint Detection and Response Expert (on-premise) oder mit der Komponente Kaspersky Endpoint Detection and Response (KATA) verwendet die Anwendung die *Regeln der Ausführungsprävention für Objekte aus 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 Verwendung der Regeln der in der Komponente EDR Expert (on-premise) enthaltenen Ausführungsprävention für Objekte über die Web Console, die Verwaltungskonsole oder die Befehlszeile aktivieren und deaktivieren.

  Wenn eine Regel der Ausführungsprävention ausgelöst wird, sendet Kaspersky Endpoint Security einen Bericht an Kaspersky 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 mit den Regeln der Ausführungsprävention für Objekte aus EDR Expert (on-premise) in der Befehlszeile anzeigen.

Funktionen der Ausführungsprävention von Objekten bei einer 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 auch im Fenster mit den Alarmdetails automatisch Regeln zur Ausführungsprävention erstellen.

Bei der Integration mit Kaspersky Endpoint Detection and Response Optimum können Sie Folgendes tun:

- Die Anwendung der Regeln der in der Komponente EDR Optimum enthaltenen Ausführungsprävention für Objekte über die Web Console oder die Befehlszeile aktivieren und deaktivieren.
- Die Regeln der Ausführungsprävention für Objekte der Komponente "EDR Optimum" in der Web Console erstellen und konfigurieren.

  Sie können auch automatisch eine Regel zur Ausführungsprävention eines Objekts erstellen, indem Sie den Start der Datei im Fenster mit den Alarmdetails verbieten. 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. Dieser Modus ist standardmäßig ausgewählt.

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.

Ausführungsprävention für Objekte in der Web Console konfigurieren

Konfiguration der Ausführungsprävention für Objekte von EDR Expert (on-premise)

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-premise)**) aktivieren oder deaktivieren.

Der Umschalter **Ausführungsprävention** aktiviert oder deaktiviert die Verwendung der Regeln der Ausführungsprävention der Komponente "EDR Expert (on-premise)".

Konfiguration der Ausführungsprävention für Objekte EDR Optimum.

Wenn die Integration mit Kaspersky Endpoint Detection and Response Optimum aktiviert ist, können Sie die Ausführungsprävention von Objekten aktivieren und deaktivieren sowie Regeln für die Ausführungsprävention von Objekten in der Komponente EDR Optimum konfigurieren:

- In den Richtlinieneigenschaften (**Anwendungsparameter** → Konfiguration der integrierten Agenten → **Endpoint Detection and Response**)
- In den Eigenschaften verwalteter Geräte (**Assets (Geräte)** → **Verwaltete Geräte** → Link <Gerätename> → Registerkarte **Anwendungen** → Link <Name des Kaspersky Endpoint Security-Programms> → Registerkarte **Programmeinstellungen** → Abschnitt **Detection and Response** → **Endpoint Detection and Response Optimum**).

Das Aktivieren und Deaktivieren der Ausführungsprävention von Objekten ist in den Geräteeigenschaften nicht verfügbar, wenn das Gerät durch eine Richtlinie verwaltet wird ist.

Parameter der Ausführungsprävention für Objekte der Komponente "EDR Optimum" in den Geräteeigenschaften

Einstellung	Description
Ausführungsprävention für Objekte aktiviert/deaktiviert	Aktiviert oder deaktiviert die Anwendung der Regeln der Ausführungsprävention der Komponente "EDR Optimum". Standardmäßig ist die Anwendung der Regeln deaktiviert.
Aktion beim Starten oder Öffnen eines Objekts	Sie können den Ausführungsmodus der Ausführungsprävention für Objekte auswählen: • **Blockieren**. In diesem Modus blockiert die App 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 App 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.
Liste mit den Regeln zur Ausführungsprävention für Objekte	Der Link **Hinzufügen** öffnet ein Fenster, in dem Sie eine Regel zur Ausführungsprävention für Objekte der Komponente "EDR Optimum" konfigurieren können. Bei Bedarf können Sie eine Regel über die Schaltfläche **Löschen** aus der Liste entfernen.

So fügen Sie der Liste eine Regel zur Ausführungsprävention für Objekte der Komponente "EDR Optimum" in den Geräteeigenschaften hinzu:

1. Klicken Sie auf die Schaltfläche **Hinzufügen** oberhalb der Liste mit den Regeln zur Ausführungsprävention von Objekten.

2. Geben Sie im folgenden Fenster den Namen der Regel zur Ausführungsprävention ein.

3. Geben Sie den Ausführungsstatus der Regel zur Ausführungsprävention an, indem Sie den Umschalter auf die entsprechende Position setzen:

   - **Aktiviert** – Die Regel ist aktiviert, und die Anwendung wendet diese Regel an.

   - **Deaktiviert** – Die Regel ist deaktiviert und wird während der Ausführung der Anwendung nicht angewendet.

   Sie können die erstellte Regel jederzeit aktivieren oder deaktivieren.

4. Wählen Sie in der Dropdown-Liste **Typ** den Objekttyp aus, den Sie blockieren möchten.

   - **Ausführbare Datei**

   - **Skript**

   - **Datei einer Office-Anwendung**

   Wenn Sie den falschen Objekttyp auswählen, wird die Datei oder das Skript nicht blockiert.

5. Um ein Objekt hinzuzufügen, geben Sie den Pfad zum Objekt und/oder die Prüfsumme des Objekts an.

   Um den Pfad zu einem Objekt anzugeben, wählen Sie die Option **Pfad verwenden** und geben Sie den Pfad zum Objekt ein.

   Um die Prüfsumme eines Objekts anzugeben, wählen Sie die Option **SHA256** oder **MD5** und geben Sie die Prüfsumme des Objekts ein.

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

   Die erstellte Regel wird zur Liste der Regeln im Parameterblock **Ausführungsprävention von Objekten** hinzugefügt.

Ausführungsprävention für Objekte in der Verwaltungskonsole konfigurieren

Sie können die Ausführungsprävention für Objekte in der Verwaltungskonsole nur aktivieren und 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 (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Programmeinstellungen** → **Detection and Response** → **EDR Expert (on-premise)**).

Das Kontrollkästchen **Ausführungsprävention für Objekte aktivieren** im Einstellungsblock **Ausführungsprävention für Objekte** aktiviert oder deaktiviert die Anwendung der Regeln der Ausführungsprävention für Objekte der Komponente EDR Expert (on-premise).

Ausführungsprävention für Objekte über die Befehlszeile konfigurieren

Über die Befehlszeile können Sie die Anwendung der Regeln zur Ausführungsprävention für Objekte mithilfe der folgenden vordefinierten Aufgaben starten und beenden:

- *Ausführungsprävention für Objekte (EDR Expert (on-premise))* (*KATAEDR_Prevention*).
- *Ausführungsprävention für Objekte (EDR Optimum)* (*EDRO_Prevention*).

Standardmäßig werden die Aufgaben *Ausführungsprävention für Objekte (EDR Expert (on-premise))* und *Ausführungsprävention für Objekte (EDR Optimum)* nicht gestartet. Sie können diese Aufgaben manuell starten und beenden.

Sie können die Aufgabe *Ausführungsprävention für Objekte (EDR Expert (on-premise))* nur starten, 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 Aufgabe *Ausführung von Objekten blockieren (EDR Optimum)* nur ausführen, wenn die Integration mit Kaspersky Endpoint Detection and Response Optimum aktiviert ist.

Mithilfe der Befehle zum Verwalten von Regeln der Ausführungsprävention für Objekte können Sie für die Komponenten EDR Expert (on-premise) und EDR Optimum eine Liste mit den Regeln der Ausführungsprävention für Objekte anzeigen.

Um die Liste mit den Regeln der Ausführungsprävention für Objekte für die Komponente EDR Expert (on-premise) anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control [-T] --get-prevention-state --kata
```

Um die Liste mit den Regeln der Ausführungsprävention für Objekte für die Komponente EDR Optimum anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control [-T] --get-prevention-state --edro
```

Cloud Sandbox

Cloud Sandbox ist eine Technologie, mit der komplexe Bedrohungen auf Ihrem Gerät 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. Anschließend werden Daten über diese Dateien an Kaspersky Security Network weitergeleitet. Wenn Cloud Sandbox also eine bösartige Datei erkennt, ergreift Kaspersky Endpoint Security Maßnahmen, um die Bedrohung auf allen Geräten zu beseitigen, auf denen diese Datei erkannt wird.

Um die Cloud Sandbox nutzen zu können, muss die Verwendung von Kaspersky Security Network aktiviert sein.

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 Lizenz, unter der Sie die Anwendung verwenden.

Wenn Sie Kaspersky Endpoint Detection and Response Optimum bereitgestellt haben, können Sie in der Web Console einen separaten Zähler für Bedrohungen aktivieren, die mit Cloud Sandbox erkannt wurden.

- In den Richtlinieneigenschaften (**Anwendungsparameter** → **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response**)
- In den Eigenschaften verwalteter Geräte (**Assets (Geräte)** → **Verwaltete Geräte** → Link <Gerätename> → Registerkarte **Anwendungen** → Link <Name des Kaspersky Endpoint Security-Programms> → Registerkarte **Programmeinstellungen** → Abschnitt **Detection and Response** → **Endpoint Detection and Response Optimum**).

Die Anzahl der von Cloud Sandbox erkannten Bedrohungen wird auch in den Berichten auf der grafischen Benutzeroberfläche angezeigt. Anhand der Daten dieses Zählers können Sie bei der Analyse erkannter Bedrohungen Statistiken erstellen.

So aktivieren Sie den Zähler für Cloud Sandbox in der Web Console in den Geräteeinstellungen:

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

   Die Liste mit Richtlinien wird geöffnet.

2. Wählen Sie die Administrationsgruppe aus, die 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. Aktivieren Sie im neuen Fenster im Parameterblock **Cloud Sandbox** den Umschalter **Cloud Sandbox**.
8. Klicken Sie auf die Schaltfläche **OK**.

Integration mit Kaspersky Unified Monitoring and Analysis Platform

Die Anwendung Kaspersky Endpoint Security ist mit der Lösung Kaspersky Unified Monitoring and Analysis Platform (im Folgenden auch "KUMA" genannt) kompatibel.

Kaspersky Unified Monitoring and Analysis Platform ist eine umfassende Softwarelösung mit den folgenden Funktionen:

- Empfang, Verarbeitung und Speicherung von Ereignissen zur Informationssicherheit (Telemetriedaten).
- Analyse und Zuordnung eingehender Daten.
- Durchsuchen der empfangenen Ereignisse.
- Erstellen von Benachrichtigungen über erkannte Anzeichen von Informationssicherheitsbedrohungen.

Weitere Informationen über diese Lösung finden Sie in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform.

Während der Integration mit Kaspersky Unified Monitoring and Analysis Platform stellen Geräte, auf denen Kaspersky Endpoint Security ausgeführt wird, verschlüsselte Verbindungen mit dem KUMA-Server her. Um die Sicherheit dieser Verbindung zu gewährleisten, werden die folgenden vom KUMA-Server ausgestellten Zertifikate verwendet:

- Zertifikat des KUMA-Servers. Die Verbindung wird mit dem TLS-Zertifikat des Servers verschlüsselt. Sie können die Sicherheit der Verbindung erhöhen, indem Sie in Kaspersky Endpoint Security die Überprüfung des Serverzertifikats aktivieren. Dafür müssen Sie vor dem Aktivieren der Integration mit Kaspersky Unified Monitoring and Analysis Platform das Zertifikat des KUMA-Servers hinzufügen.
- Client-Zertifikat. Dieses Zertifikat dient dem zusätzlichen Schutz der Verbindung durch die Zwei-Wege-Authentifizierung (Überprüfung der Geräte, auf denen Kaspersky Endpoint Security installiert ist, durch den KUMA-Server). Mehrere Geräten können dasselbe Client-Zertifikat verwenden. Standardmäßig überprüft der KUMA-Server keine Client-Zertifikate, die Zwei-Wege-Authentifizierung kann jedoch auf der Seite von Kaspersky Unified Monitoring and Analysis Platform aktiviert werden. In diesem Fall müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen für die Integration mit Kaspersky Unified Monitoring and Analysis Platform aktivieren und ein Client-Zertifikat hinzufügen (ein Crypto-Container mit einem Zertifikat und einem privaten Schlüssel).

Zertifikate für die Absicherung der Verbindung zum KUMA-Server werden vom Administrator für Kaspersky Unified Monitoring and Analysis Platform bereitgestellt.

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.

Die Integration mit Kaspersky Unified Monitoring and Analysis Platform ist standardmäßig deaktiviert. Sie können die Integration aktivieren und deaktivieren und die folgenden Einstellungen für die Integration über die Befehlszeile, in der Web Console und mithilfe der Verwaltungskonsole konfigurieren:

- Allgemeine Einstellungen für die Verbindung mit den KUMA-Servern konfigurieren.
- Zertifikate für KUMA-Server hinzufügen oderentfernen.
- Die Zwei-Wege-Authentifizierung beim Herstellen einer Verbindung mit den KUMA-Servern konfigurieren und Client-Zertifikate hinzufügen.
- Einstellungen für die Übertragung von Ereignissen konfigurieren.

Stellen Sie vor der Aktivierung der Integration mit der Kaspersky Unified Monitoring and Analysis Platform sicher, dass eine der folgenden Bedingungen erfüllt ist:

- Sie verwenden Kaspersky Endpoint Security unter einer Lizenz, welche die Funktionalitäten von Kaspersky Unified Monitoring and Analysis Platform abdeckt.
- Sie haben eine separate Lizenz zur Nutzung der Funktionalitäten von der Kaspersky Unified Monitoring and Analysis Platform erworben und einen Lizenzschlüssel für zusätzliche Funktionen (KUMA-Schlüssel) in der Anwendung hinzugefügt.

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

Integration mit KUMA in der Web Console konfigurieren

In der Web Console können Sie die Einstellungen der Integration mit der Anwendung "Kaspersky Unified Monitoring and Analysis Platform" in den Richtlinieneigenschaften konfigurieren (**Anwendungseinstellungen → Konfiguration der integrierten Agenten → KUMA-Integration**).

Integration mit KUMA in der Verwaltungskonsole konfigurieren

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 (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**KUMA-Integration → KUMA-Integration**).

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 dem KUMA-Server

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 zum KUMA-Server: TCP oder UDP. 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 Einstellungen für Verbindungen mit KUMA-Servern konfigurieren.

Einstellungen für die Verbindung mit dem KUMA-Server

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.
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 Zwei-Wege-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.
Zwei-Wege-Authentifizierung verwenden	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 Zwei-Wege-Authentifizierung aktiviert sein.

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. Wenn das Archiv durch ein Kennwort geschützt ist, geben Sie das Kennwort in das Feld **Kennwort des Crypto-Containers** ein.

Integration mit KUMA über die Befehlszeile konfigurieren

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.

Einstellungen der 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* festlegen können.

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.		
`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. `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 **[SiemTransferSettings]** enthält Parameter 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`.

Verwaltung der Zertifikate für die Verbindung mit dem KUMA-Server

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 <Dateipfad>
```

wobei `<Dateipfad>` dem Pfad der DER- oder PEM-Datei entspricht, die das Serverzertifikat enthält.

Um ein Client-Zertifikat hinzuzufügen oder zu ersetzen:

1. Führen Sie den Befehl aus:

   ```
   kesl-control [-M] --add-kuma-client-certificate <Dateipfad>
   ```

   Wobei `<Dateipfad>` dem Namen und Pfad des Crypto-Containers (Archiv im pfx-Format) entspricht, der den geheimen Schlüssel enthält.

2. Wenn der Crypto-Container durch ein Kennwort geschützt ist, geben Sie das Kennwort ein, wenn Sie dazu aufgefordert werden.

Das Client-Zertifikat wird verwendet, um die Verbindung zum 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 ein Serverzertifikat:

  ```
  kesl-control [-M] --query-kuma-server-certificate
  ```

- Für ein 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
```

Einstellungen zur Verwendung der Anwendung im Light Agent-Modus konfigurieren

Die in diesem Abschnitt beschriebenen Einstellungen können nur angewendet werden, wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird.

Um Kaspersky Endpoint Security im Light Agent-Modus auszuführen, ist eine permanente Interaktion zwischen dem Light Agent und dem auf der SVM installierten Schutzserver erforderlich. Wenn keine Verbindung zum Schutzserver besteht, kann der Light Agent keine Dateifragmente zur Untersuchung an den Schutzserver übertragen und es findet keine Untersuchung statt.

Um mit dem Schutzserver zu interagieren, stellt der Light Agent zu der SVM mit dem installierten Schutzserver eine Verbindung her und erhält diese aufrecht.

Sie können die Einstellungen für die Verbindung des Light Agent mit der SVM in der Web Console oder in der Verwaltungskonsole konfigurieren. Über die Befehlszeile können keine Einstellungen konfiguriert werden; Sie können nur Informationen zur Verwendung der Anwendung im Light Agent-Modus anzeigen.

Sie können die folgenden Parameter für die Verbindung von Light Agent mit SVM konfigurieren:

- Methode der SVM-Erkennung. Sie können die Methode auswählen, die von den Light Agents verwendet werden soll, um verfügbare SVMs zum Herstellen einer Verbindung zu erkennen. Der Light Agent kann SVMs, die im Netzwerk ausgeführt werden, auf eine der folgenden Arten erkennen:
  - Mittels des Integrationsservers. SVMs übermitteln Informationen über sich selbst an den Integrationsserver. Der Integrationsserver generiert eine Liste der für die Verbindung verfügbaren SVMs und stellt diese den Light Agents zur Verfügung.

    Um diese Methode der SVM-Erkennung verwenden zu können, müssen die SVMs und Light Agents mit dem Integrationsserver verbunden sein.

    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.
  - Mittels einer Liste von SVM-Adressen. Sie können eine Liste mit SVM-Adressen angeben, zu denen die Light Agents eine Verbindung herstellen können.
- Algorithmus zur SVM-Auswahl für die Verbindung. Nachdem der Light Agent Informationen über verfügbare SVMs erhalten hat, wählt er gemäß dem Algorithmus zur SVM-Auswahl die optimale SVM für die Verbindung aus. Sie können angeben, welchen Algorithmus die Light Agents verwenden sollen, wenn sie eine SVM für die Verbindung auswählen.

- Tags der Verbindung. Sie können die Verbindung von Light Agents zur SVM mithilfe von Tags für die Verbindung regulieren. Wenn Sie für eine Verbindung Tags verwenden, kann der Light Agent nur eine Verbindung zu den SVMs herstellen, auf denen die Verwendung dieses Tags zur Verbindung konfiguriert ist.

- Schutz der Verbindung zwischen dem Light Agent und dem Schutzserver. Sie können die Verbindung zwischen Light Agents und Schutzservern durch Verschlüsselung schützen.

Weitere Informationen zu den Verbindungseinstellungen zwischen einem Light Agent und SVMs finden Sie in der Hilfe der zu Kaspersky Security for Virtualization Light Agent.

Light Agent-Einstellungen in der Web Console konfigurieren

In der Web Console können Sie die Einstellungen für die Verbindung des Light Agents mit SVMs in den Richtlinieneigenschaften verwalten (**Programmeinstellungen** → **Light Agent-Modus**).

Light Agent-Einstellungen in der Verwaltungskonsole konfigurieren

In der Verwaltungskonsole können Sie die Einstellungen für die Verbindung des Light Agents mit SVMs in den Richtlinieneigenschaften verwalten (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Light Agent-Modus**).

Verbindung zum Integrationsserver

Die in diesem Abschnitt beschriebenen Einstellungen können nur angewendet werden, wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird.

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

In diesem Fenster werden die aktuellen Parameter für die Verbindung von Light Agents mit dem Integrationsserver angezeigt: Adresse und Port für die Verbindung. Durch Klicken auf die Schaltfläche **Ändern** öffnet sich das Fenster **Verbindung zum Integrationsserver**, in dem Sie die Verbindung zum Integrationsserver konfigurieren können.

Fenster "Verbindung zum Integrationsserver"

In diesem Fenster können Sie die Parameter für die Verbindung von Light Agents mit dem Integrationsserver festlegen oder ändern.

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 Integrationsserver mittels Administratorrechten hergestellt wurde, wird das Kennwort Benutzerkontos `agent` automatisch in die Richtlinie übertragen, die zur Verbindung von Light Agents mit dem Integrationsserver verwendet wird.

Einstellungen der SVM-Erkennung

Die in diesem Abschnitt beschriebenen Einstellungen 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 jedes Zeichen mit Ausnahme von `;` 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 virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, Skala-R, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, 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-Plattform, VK Cloud (VK Private Cloud) oder der TIONIX Cloud Platform betrieben wird).
	  Wenn auf demselben Hypervisor oder in derselben Servergruppe, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her.
	• **Cluster**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):
	  • Die SVM wird auf demselben Hypervisor-Cluster bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, Skala-R, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).
	  • Die SVM wird in demselben OpenStack-Projekt bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack-Plattform, VK Cloud (VK Private Cloud) oder der TIONIX Cloud Platform betrieben wird).
	  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 Datencenter bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, Skala-R, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, 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, VK Cloud (VK Private Cloud) oder der TIONIX Cloud Platform betrieben wird).
	  Wenn in demselben Datencenter 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.

Informationen zur Verwendung der Anwendung im Light Agent-Modus über die Befehlszeile anzeigen

In der Befehlszeile können Sie die folgenden Informationen zur Verwendung der Anwendung im Light Agent-Modus zum Schutz virtueller Umgebungen anzeigen:

- Einstellungen zur Verwendung der Anwendung im Light Agent-Modus;
- Verbindung des Light Agents zum Integrationsserver;
- Verbindung des Light Agents zur SVM.

Um Informationen zu den Einstellungen für die Verwendung der Anwendung im Light Agent-Modus anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control [-V] --ksvla-info
```

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

- Light Agent-Modus zum Schutz virtueller Umgebungen: aktiviert/deaktiviert.

  Wenn der Light Agent-Modus aktiviert ist, wird die Anwendung als Light Agent im Rahmen von Kaspersky Security for Virtualization Light Agent verwendet.

- Modus zum Schutz der VDI-Infrastruktur: aktiviert/deaktiviert.

  Der Modus zum Schutz der VDI-Infrastruktur optimiert die Ausführung von Kaspersky Endpoint Security auf temporären virtuellen Maschinen. Wenn der Modus zum Schutz der VDI-Infrastruktur aktiviert ist, werden Updates, die einen Neustart der geschützten virtuellen Maschine erfordern, nicht auf temporären virtuellen Maschinen installiert. Wenn Updates eingehen, die einen Neustart erfordern, sendet der auf einer temporären virtuellen Maschine installierte Light Agent eine Nachricht an Kaspersky Security Center über die Notwendigkeit, das Template der geschützte virtuellen Maschinen zu aktualisieren.

- Typ der geschützten virtuellen Maschine: temporär oder permanent.

- Rolle der geschützten virtuellen Maschine in der virtuellen Infrastruktur: Server oder Workstation.

- ID/Identifikator (UUID) der geschützten virtuellen Maschine.

Um Informationen zur Verbindung des Light Agents mit dem Integrationsserver anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control [-V] --viis-info
```

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

- Adresse und der Port des Integrationsservers, mit dem sich der Light Agent verbindet.

  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 von Kaspersky Security for Virtualization Light Agent.

- Status der Verbindung zum Integrationsserver.

- Datum und Uhrzeit der letzten Verbindung zwischen dem Light Agent und dem Integrationsserver.

Um Informationen zur Verbindung des Light Agents mit der SVM anzuzeigen, führen Sie den folgenden Befehl aus:

```
kesl-control [-V] --svm-info
```

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

- Die Adresse der SVM, mit welcher der Light Agent verbunden ist, und der SVM-Standort in der virtuellen Infrastruktur relativ zum Light Agent: lokal oder nicht lokal.

- Methode 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.

Ereignisse und Berichte anzeigen

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 die Anwendung die Informationen über Ereignisse in der Datenbank /var/opt/kaspersky/kesl/private/storage/events.db. 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. Nähere Informationen zu Ereignissen finden Sie in der Hilfe zu Kaspersky Security Center.

Sie können Informationen zu Anwendungsereignissen auf folgende Arten abrufen:

- In der Verwaltungskonsole und in der Web Console.

- Über die Befehlszeile (Ereignisse über die Befehlszeile anzeigen, Ereignisse in Kaspersky Security Center anzeigen)

- Über die grafischen Benutzeroberfläche der Anwendung in den Pop-up-Benachrichtigungen, wenn die Anzeige von Benachrichtigungen in den Richtlinieneigenschaften oder in den allgemeinen Anwendungseinstellungen 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. Nähere Informationen über die Verwendung der Berichte von Kaspersky Security Center finden Sie in der Hilfe zu Kaspersky Security Center.

- In der grafischen Benutzeroberfläche von Kaspersky Endpoint Security sind Berichte verfügbar, die Auskunft über den Betrieb der Anwendung und über ihre Komponenten und Aufgaben geben.

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'` sind zwei Zeichen (Backslash + a)

`'\\'` ist ein Zeichen (Backslash).

`'\\\\'` besteht aus 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 aufgezeichnet werden. Sie können die Aufzeichnung von Ereignissen in diesem Protokoll über die Web Console, die Verwaltungskonsole oder die Befehlszeile aktivieren oder deaktivieren.

Wenn Sie die Befehlszeile zur Verwaltung der Anwendung verwenden, ist die Protokollierung von Ereignissen im Protokoll des Betriebssystems standardmäßig deaktiviert.

Wenn Sie Kaspersky Endpoint Security im Standard-Modus oder im Modus als Endpoint Detection and Response Agent verwenden und die Anwendung mittels Kaspersky Security Center verwalten, werden im Protokoll des Betriebssystems standardmäßig Informationen über das Hinzufügen und Entfernen von Lizenzschlüsseln sowie über den Ablauf der Lizenz aufgezeichnet. In den Richtlinieneigenschaften, unter denen die Anwendung ausgeführt wird, können Sie die Ereignisse auswählen, die in das Protokoll des Betriebssystems geschrieben werden.

Konfiguration in der Web Console

In der Web Console können Sie in den Richtlinieneigenschaften (**Programmeinstellungen** → **Allgemeine Einstellungen** → **Ereigniseinstellungen**) die Protokollierung von Ereignissen im Protokoll des Betriebssystems aktivieren oder deaktivieren.

Wenn Sie im Block mit dem Namen der Ereigniskategorien (kritische Ereignisse, Funktionsfehler, Warnung, Info-Meldung) auf die Schaltfläche **Einstellungen** klicken, öffnet sich ein Fenster, das eine Liste mit den Ereignissen der entsprechenden Ereigniskategorie enthält. Für jedes Ereignis kann die Speicherung im Protokoll des Betriebssystems konfiguriert werden.

Konfiguration in der Verwaltungskonsole

In der Verwaltungskonsole können Sie die Protokollierung von Ereignissen im Protokoll des Betriebssystems in den Richtlinieneigenschaften (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Allgemeine Einstellungen** → **Programmeinstellungen**) konfigurieren.

Der Link **Konfigurieren** im Block **Benachrichtigungen** öffnet das Fenster **Benachrichtigungseinstellungen**. In diesem Fenster können Sie mithilfe von Kontrollkästchen die Ereignisse auswählen, die von der Anwendung in Protokoll des Betriebssystems protokolliert werden soll.

Sie können einzelne Ereignistypen oder alle Ereignistypen einer bestimmten Ereigniskategorie auswählen (kritische Ereignisse, Funktionsfehler, Warnungen, Info-Meldungen).

Konfiguration 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.

Der Parameter `UseSyslog` kann folgende Werte annehmen:

- `Yes` – Protokollieren von Ereignissen im syslog aktivieren.
- `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 den Wert von Parametern mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen enthält.

Ereignisse in Kaspersky Security Center anzeigen

Eine Liste aller Ereignisse während der Ausführung von Kaspersky Endpoint Security wird in der Web Console und in der Verwaltungskonsole angezeigt.

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.

Sie können Benachrichtigungen über Ereignisse konfigurieren. Eine *Benachrichtigung* ist eine Nachricht mit Informationen über ein Ereignis, das auf einem geschützten Gerät aufgetreten ist. Mithilfe von Benachrichtigungen können Sie zeitnah über Ereignisse in der Anwendung 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 über die Befehlszeile anzeigen

Über die Befehlszeile können Sie Folgendes anzeigen:

- aktuelle Anwendungsereignisse;

- Ereignisse aus dem Ereignisprotokoll der Anwendung.

Ausgabe aktueller Ereignisse

Sie können in der Konsole Informationen zu allen aktuellen Anwendungsereignissen oder zu aktuellen Ereignissen im Zusammenhang mit dem Starten oder Beenden einer bestimmten Aufgabe anzeigen. Über einen Filter können Sie sich auch bestimmte aktuelle Ereignisse anzeigen lassen, beispielsweise Ereignisse eines bestimmten Typs.

Um Informationen zu allen aktuellen Anwendungsereignissen in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
Befehl kesl-control -W
```

Der Befehl gibt den Namen des Ereignisses und zusätzliche Informationen über das Ereignis zurück.

Um in die Konsole nur Informationen zu aktuellen Ereignissen, die mit der ausgeführten Aufgabe verknüpft sind, auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control --start-task <ID/Name der Aufgabe> -W
```

Beispiel:
Ausgabe der aktuellen Ereignisse der gestarteten Aufgabe mit ID=1 aktivieren:

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

Um Informationen zu aktuellen Ereignissen, die den Filterkriterien entsprechen, in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control -W --query "<Filterbedingungen>"
```

Filterbedingungen werden mit einem oder mehreren logischen Ausdrücken im Format `<Feld>` `<Vergleichsoperator>` `'<Wert>'` festgelegt, die mit dem logischen Operator `and` kombiniert werden.

Beispiel:
Ausgeben der Ereignisse vom Typ "TaskStateChanged":

```
kesl-control -W --query "EventType == 'TaskStateChanged'"
```

Ausgeben der Ereignisse vom Typ "TaskStateChanged", die vom Benutzer "User" angestoßen wurden.

```
kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'"
```

Ereignisse aus dem Ereignisprotokoll ausgeben

Sie können Informationen zu Ereignissen aus dem Ereignisprotokoll der Anwendung in die Konsole oder in eine Datei ausgeben. Sie können einen Filter verwenden, um bestimmte Ereignisse auszugeben.

Um Informationen zu allen Ereignissen im Ereignisprotokoll der Anwendung in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control -E --query [--db <Datenbankdatei>]
```

wobei `<Datenbankdatei>` den vollständigen Pfad zur Datenbankdatei des Ereignisprotokolls, aus dem Sie Ereignisse ausgeben möchten, darstellt. Standardmäßig speichert die Anwendung 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.

Wenn sich das Ereignisprotokoll in der Standarddatenbank befindet, können Sie in der Konsole die Informationen zu allen Ereignissen mittels des Befehls `kesl-control -E` ausgeben.

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.

Um Informationen zu Ereignissen im Ereignisprotokoll der Anwendung, die bestimmten Bedingungen entsprechen, in die Konsole auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control -E --query "<Filterbedingungen>" [--db <Datenbankdatei>] [-n <Anzahl>]
[--json] [--reverse]
```

wobei:

- Mit `<Filterbedingungen>` werden ein oder mehrere logische Ausdrücke im Format `<Feld> <Vergleichsoperation> '<Wert>'` angegeben, die mit dem logischen Operator `and` kombiniert werden, um Abfrageergebnisse einzuschränken.
- `<Anzahl>` ist die Anzahl der letzten Ereignisse aus der Auswahl (Einträge, gezählt ab dem Ende der Auswahl), die angezeigt werden sollen.
- `--json` – Gibt die Ereignisse im JSON-Format aus.
- `--reverse` – Ereignisse in umgekehrter Reihenfolge anzeigen (das neueste Ereignis steht oben und das ältesten unten).

Um Informationen zu Ereignissen im Ereignisprotokoll der Anwendung, die bestimmten Bedingungen entsprechen, in eine Datei auszugeben, führen Sie den folgenden Befehl aus:

```
kesl-control -E --query "<Filterbedingungen>" [--db <Datenbankdatei>] [-n <Anzahl>] -
-file <Dateipfad> [--json]
```

Wobei `--file <Dateipfad>` dem vollständigen Pfad zu der Datei entspricht, in die Sie die Ereignisse ausgeben möchten.

Einstellungen für Pop-up-Benachrichtigungen über die grafische Benutzeroberfläche konfigurieren

In der grafischen Benutzeroberfläche der Anwendung werden Informationen über Ereignisse standardmäßig in Pop-up-Benachrichtigungen angezeigt. Sie können das Anzeigen von Pop-up-Benachrichtigungen mittels Verwaltungskonsole oder Befehlszeile aktivieren und deaktivieren.

Konfiguration in der Verwaltungskonsole

In der Verwaltungskonsole können Sie in den Richtlinieneigenschaften die Anzeige von Popup-Benachrichtigungen in der grafischen Benutzeroberfläche aktivieren oder deaktivieren (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Allgemeine Einstellungen** → **Programmeinstellungen**).

Das Kontrollkästchen **Pop-up-Benachrichtigungen in der grafischen Benutzeroberfläche anzeigen** aktiviert das Anzeigen von Pop-up-Benachrichtigungen in der grafischen Benutzeroberfläche.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Konfiguration 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 des Parameters mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen enthält.

Der Parameter `ShowPopUpNotifications` kann folgende Werte annehmen:

- `Yes` (Standardwert) – In der grafischen Benutzeroberfläche werden Pop-up-Benachrichtigungen angezeigt.
- `No` – In der grafischen Benutzeroberfläche werden keine Pop-up-Benachrichtigungen angezeigt.

App über die grafische Benutzeroberfläche verwalten

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

Mit der grafischen Oberfläche von Kaspersky Endpoint Security können Sie Folgendes tun:

- Informationen zum Schutzstatus des Geräts anzeigen.
- Anwendungskomponenten aktivieren oder deaktivieren:
  - 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 BadUSB-Angriffen.
  - Verhaltensanalyse.
  - Exploit-Prävention.
  - Programmkontrolle.
  - Web-Kontrolle.
  - Überwachung der System-Integrität.
- Untersuchungsaufgaben starten und beenden:
  - Schadsoftware-Untersuchung.
  - Untersuchung wichtiger Bereiche.
  - Untersuchung von Containern.
- Benutzerdefinierte Untersuchung von Dateien und Verzeichnissen starten.

- Aufgaben zum Rollback des Datenbanken-Updates starten und beenden.
- Datei oder Verzeichnis zur Untersuchung an Sandbox senden.
- Die Verwendung von Kaspersky Security Network aktivieren und deaktivieren.
- Lizenzschlüssel der Anwendung verwalten und Informationen zur Lizenz, unter der die Anwendung verwendet wird, und zu dem mit der Lizenz verknüpften Schlüssel anzeigen.
- Beim Administrator des lokalen Netzwerks der Organisation temporären Zugriff auf ein blockiertes Gerät anfordern und erhalten.
- Ausführungsstatistik der Anwendung und Berichte anzeigen.
- Informationen zu Objekten anzeigen, die im Backup abgelegt wurden.
- Protokolldateien der Anwendung erstellen.

Wenn die App im EDR-Agent-Modus verwendet wird, ist nur eine begrenzte Auswahl an App-Komponenten 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“.

Wenn eine Komponente oder Aufgabe der Anwendung im informativen Modus ausgeführt wird, zeigt die grafische Oberfläche der Anwendung für diese Komponente oder Aufgabe die Warnung *Informativer Ausführungsmodus ausgewählt* an.

Grafische Oberfläche

Anwendungssymbol 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 12.4 für Linux**. Öffnet das Hauptfenster der grafischen Oberfläche der Anwendung. Dieses Fenster zeigt den Schutzstatus Ihres Geräts an und enthält Elemente der Oberfläche, die den Zugriff auf die Funktionen der Anwendung ermöglichen.
- **Beenden**. Beendet die grafische Benutzeroberfläche.

Hauptfenster der grafischen Oberfläche der Anwendung

Sie können das Hauptfenster der grafischen Oberfläche der Anwendung auf eine der folgenden Arten öffnen:

- Wählen Sie den Anwendungsnamen im Menü des Fenstermanagers des Betriebssystems.
- Klicken Sie mit der rechten Maustaste oder doppelklicken Sie auf das Anwendungssymbol im Infobereich der Taskleiste.

Das Hauptfenster der grafischen Oberfläche der Anwendung ist in mehrere Bereiche unterteilt:

- Der obere Bereich des Hauptfensters wird der Schutzstatus des Geräts angezeigt. Durch Anklicken der Schaltfläche **Anzeigen** wird das Fenster **Schutz-Center** geöffnet. In diesem Fenster werden Informationen zum Schutzstatus des Geräts sowie Empfehlungen zu Maßnahmen angezeigt, die Sie gegebenenfalls zur Behebung von Problemen im Schutz ergreifen müssen.

- Der Block **Untersuchung** zeigt den Status der Aufgabe zur Schadsoftware-Untersuchung und die Anzahl der gefundenen Bedrohungen an. Durch Anklicken dieses Blocks wird das Fenster **Untersuchung** geöffnet. In diesem Fenster können Sie die Aufgaben *Schadsoftware-Untersuchung*, *Untersuchung wichtiger Bereiche* und *Untersuchung von Containern* starten und beenden. Außerdem können Sie Berichte zu diesen Aufgaben anzeigen.

- Der Block **Update** zeigt den Status der *Update-Aufgabe* an. Durch Anklicken dieses Blocks wird das Fenster **Update** geöffnet. In diesem Fenster können Sie die *Update*-Aufgabe und das *Rollback des Datenbanken-Updates* starten. Außerdem können Sie Berichte zu diesen Aufgaben anzeigen.

- Im unteren Bereich des Hauptfensters befinden sich die folgenden Elemente:

  - Die Schaltfläche **Berichte**. Diese Schaltfläche öffnet das Fenster **Berichte**, in dem Sie die Ausführungsstatistik der Komponenten und Aufgaben sowie diverse Berichte anzeigen können.

  - Die Schaltfläche **Backup**. Diese Schaltfläche öffnet das Fenster **Backup**, das Informationen zu Objekten im Backup enthält.

  - Schaltfläche **Einstellungen**. Diese Schaltfläche öffnet das Fenster **Einstellungen**, in dem Sie die Komponenten der Anwendung und die Verwendung von Kaspersky Security Network aktivieren und deaktivieren können.

  - Schaltfläche **Temporärer Zugriff**. Durch Klicken auf diese Schaltfläche wird das Fenster **Temporärer Zugriff** geöffnet, in dem Sie temporären Zugriff auf das gesperrte Gerät anfordern und erhalten können.

  - Die Schaltfläche **Support**. Diese Schaltfläche öffnet das Fenster **Support**, in dem Sie sowohl Informationen zur Anwendung anzeigen als auch eine Protokolldatei für die Anwendung erstellen können.

- Im untersten Teil des Hauptfensters der Anwendung werden Informationen zur Lizenz und zum Schlüssel sowie zu etwaigen Problemen mit der Lizenz angezeigt. Diese Schaltfläche öffnet das Fenster **Lizenzen**, in dem detaillierte Informationen zur Lizenz angezeigt werden. Wenn Sie in diesem Fenster auf die Schaltfläche **Lizenz erwerben** klicken, wird die Website des Kaspersky-Onlineshops geöffnet, auf der Sie eine Lizenz erwerben können. Nach dem Erwerb einer Lizenz erhalten Sie einen Aktivierungscode oder eine Schlüsseldatei, mit der Sie die Anwendung aktivieren müssen.

Zur Verwaltung der grafischen Oberfläche sind Benutzerrechte mit Administrator-Rolle (admin) erforderlich. Benutzern mit anderen Rollen stehen einige Elemente der grafischen Oberfläche möglicherweise nicht zur Verfügung.

Anwendungskomponenten aktivieren und deaktivieren

Sie können Komponenten der Anwendung in der grafischen Benutzeroberfläche mithilfe von Umschaltern ein- und ausschalten.

Standardmäßig sind nur die Komponenten zum Schutz vor bedrohlichen Dateien, zur Gerätekontrolle und zur Verhaltensanalyse aktiviert. Die Komponente zum Schutz vor Web-Bedrohungen kann automatisch aktiviert werden, wenn auf dem Gerät die lokale Konfiguration des Schutzes vor Web-Bedrohungen aktiviert ist (d. h. es wird keine Richtlinie angewendet oder die Richtlinieneigenschaften werden nicht durch das "Schloss" gesperrt) und auf dem System einer der unterstützten Browser erkannt wird.

So aktivieren oder deaktivieren Sie eine Anwendungskomponente:

1. Öffnen Sie das Hauptfenster der grafischen Oberfläche der Anwendung.
2. Klicken Sie im unteren Bereich des Hauptfensters auf die Schaltfläche **Einstellungen**.

   Das Fenster **Einstellungen** wird geöffnet.
3. Schalten Sie den Umschalter für die gewünschte Komponente ein oder aus.

Untersuchungsaufgaben starten und beenden

So starten oder stoppen Sie eine Untersuchungsaufgabe:

1. Öffnen Sie das Hauptfenster der grafischen Oberfläche der Anwendung.
2. Klicken Sie im Hauptfenster auf die Schaltfläche **Untersuchung**.

   Das Fenster **Untersuchung** wird geöffnet.
3. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie eine Untersuchungsaufgabe starten möchten, klicken Sie auf die Schaltfläche **Starten** unterhalb der entsprechenden Untersuchungsaufgabe.

     Der Fortschritt der laufenden Untersuchungsaufgabe wird angezeigt.

   - Wenn Sie eine Untersuchungsaufgabe anhalten möchten, klicken Sie auf die Schaltfläche **Halt** unterhalb der entsprechenden Untersuchungsaufgabe.

     Die Untersuchungsaufgabe wird angehalten und es werden Informationen zu untersuchten Objekten und erkannten Bedrohungen angezeigt.
4. Wenn Sie einen Bericht über die Untersuchungsaufgabe möchten, klicken Sie auf die Schaltfläche **Bericht anzeigen**.

Wenn ein infiziertes Objekt erkannt wird oder die Untersuchungsaufgabe abgeschlossen ist, wird im Infobereich neben dem Anwendungssymbol auf der rechten Seite der Taskleiste ein Pop-up-Fenster angezeigt.

Das Fenster **Untersuchung** zeigt auch den Fortschritt und die Ergebnisse temporärer Aufgaben zur Untersuchung von Bootsektoren (*Scan_Boot_Sectors_{ID}*) und temporärer Aufgaben zur benutzerdefinierten Untersuchung von Dateien (*Scan_File_{ID}*). Sie können die Informationen zu ausgeführten temporären Aufgaben ausblenden, indem Sie auf das Kreuzchen klicken oder das Fenster **Untersuchung** schließen (beim Wechsel zum Hauptfenster oder beim Verlassen der Anwendung).

Benutzerdefinierte Untersuchung und Untersuchung in Sandbox starten

Sie können die benutzerdefinierten Untersuchungen von Dateien und Verzeichnissen über die grafische Oberfläche ausführen.

So starten Sie die benutzerdefinierte Untersuchung einer Datei oder eines Verzeichnisses:

1. Öffnen Sie das Kontextmenü, indem Sie mit der rechten Maustaste auf die zu untersuchende Datei bzw. das Verzeichnis klicken.

2. Wählen Sie **Kaspersky Endpoint Security 12.4 für Linux** als Anwendung zur Untersuchung der Datei oder des Verzeichnisses aus.

   Die Namen der Punkte im Kontextmenü kann je nach Desktop-Umgebung variieren.

Die benutzerdefinierte Untersuchungsaufgabe und der Fortschritt werden in der grafischen Oberfläche angezeigt.

Wenn die Integration von Kaspersky Endpoint Security mit Sandbox aktiviert ist, können Sie über die grafische Oberfläche eine Datei oder ein Verzeichnis zur Untersuchung an Sandbox senden.

So senden Sie eine Datei oder ein Verzeichnis zur Untersuchung an Sandbox:

1. Öffnen Sie das Kontextmenü, indem Sie mit der rechten Maustaste auf die Datei bzw. das Verzeichnis klicken, die bzw. das Sie zur Untersuchung senden möchten.

2. Wählen Sie **Kaspersky Endpoint Security 12.4 für Linux** als Anwendung zur Untersuchung der Datei oder des Verzeichnisses aus.

   Die Namen der Punkte im Kontextmenü kann je nach Desktop-Umgebung variieren.

3. Wählen Sie im nächsten Fenster die Option **An Sandbox senden** aus.

Update-Aufgabe starten und beenden

So starten oder stoppen Sie eine Update-Aufgabe:

1. Öffnen Sie das Hauptfenster der grafischen Oberfläche der Anwendung.

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 die Update-Aufgabe erfolgreich abgeschlossen wurde, wird der Link **Update-Rollback** verfügbar und Sie können ein Rollback des letzten erfolgreichen Datenbanken-Updates durchführen.

- Wenn Sie eine Aufgabe beenden möchten, klicken Sie auf **Halt** unterhalb der entsprechenden Aufgabe.

  Die Update-Aufgabe wird angehalten.

4. Wenn Sie einen Bericht über die Aufgabe anzeigen möchten, klicken Sie auf die Schaltfläche **Bericht anzeigen**.

So starten Sie eine Aufgabe zum Rollback des Updates:

1. Öffnen Sie das Hauptfenster der grafischen Oberfläche der Anwendung.
2. Klicken Sie im Hauptfenster der Anwendung auf den Abschnitt **Update**.

   Das Fenster **Update** wird geöffnet.
3. Starten Sie die Aufgabe zum Rollback des Datenbanken-Updates, indem Sie auf den Link **Update-Rollback** klicken.

Verwendung von Kaspersky Security Network konfigurieren

Sie können die Verwendung von Kaspersky Security Network über die grafische Oberfläche aktivieren oder deaktivieren.

So aktivieren Sie die Verwendung von Kaspersky Security Network:

1. Öffnen Sie das Hauptfenster der grafischen Oberfläche der Anwendung.
2. Klicken Sie im unteren Bereich des Hauptfensters auf die Schaltfläche **Einstellungen**.

   Das Fenster **Einstellungen** wird geöffnet.
3. Wählen Sie im Fenster **Einstellungen** eine der folgenden Optionen aus:

   - **Erweiterter KSN-Modus**, wenn Sie Kaspersky Security Network nutzen möchten, um Informationen aus der Wissensdatenbank abzurufen und anonyme Statistikdaten und Informationen über die Typen und Quellen der Bedrohungen zu senden.
   - **Standardmäßiger KSN-Modus**, wenn Sie Kaspersky Security Network nutzen möchten, um Informationen aus der Wissensdatenbank abzurufen, aber keine anonymen Statistikdaten und Informationen über die Typen und Quellen der Bedrohungen zu senden.
4. Klicken Sie auf die Schaltfläche **Aktivieren**.

   Das Fenster **Verwendung von Kaspersky Security Network**.
5. Lesen Sie im Fenster **Verwendung von Kaspersky Security Network** die Erklärung zu Kaspersky Security Network sorgfältig durch und wählen Sie die Option **Ich bestätige, dass ich die Bedingungen der Erklärung zu Kaspersky Security Network vollständig gelesen habe, und sie verstehe und akzeptiere.**
6. Klicken Sie auf die Schaltfläche **OK**.

   Die Schaltfläche **OK** ist nicht verfügbar, wenn im Fenster **Verwendung von Kaspersky Security Network** keine der Optionen ausgewählt ist.

So deaktivieren Sie die Verwendung von Kaspersky Security Network:

1. Öffnen Sie das Hauptfenster der grafischen Oberfläche der Anwendung.
2. Klicken Sie im unteren Bereich des Hauptfensters der Anwendung auf die Schaltfläche **Einstellungen**.

   Das Fenster **Einstellungen** wird geöffnet.
3. Klicken Sie auf die Schaltfläche **Deaktiviert**.
4. Klicken Sie im geöffneten Fenster auf **Ja**, um auf die Teilnahme an Kaspersky Security Network zu verzichten.

Berichte anzeigen

Berichte über die Ausführung der Komponenten und Aufgaben der Anwendung können Sie über die grafische Oberfläche anzeigen. Berichte werden in einem Fenster angezeigt, das durch Anklicken der Schaltfläche **Berichte** im unteren Teil des Hauptfensters der grafischen Oberfläche der Anwendung geöffnet wird.

Die Berichtdaten werden als Tabelle angezeigt, die eine Liste von Ereignissen enthält. Jede Zeile der Tabelle enthält Informationen zu einem bestimmten Ereignis. Die Ereignisattribute werden in den Tabellenspalten angezeigt. Ereignisse, die während der Ausführung verschiedener Komponenten und Aufgaben protokolliert werden, haben unterschiedliche Attribute.

Die Berichte enthalten folgende Ereigniskategorien:

- *Kritisch* – Das sind Ereignisse von kritischer Bedeutung, die Sie beachten müssen, da sie auf Probleme mit der Anwendung oder auf Schwachstellen beim Schutz Ihres Geräts hinweisen.
- *Hoch.*
- *Mittel.*
- *Niedrig.*
- *Informativ.*
- *Fehler.*

Die folgenden Berichte sind in der Anwendung verfügbar:

- **Statistik**. Dieser Bericht enthält statistische Daten zur Ausführung der Komponente "Schutz vor bedrohlichen Dateien" und den Untersuchungsaufgaben. Durch Klicken auf **Aktualisieren** können Sie den angezeigten Bericht aktualisieren.
- **Systemaudit**. Dieser Bericht enthält Informationen über Ereignisse, die bei der Ausführung der Anwendung und während der Interaktion des Benutzers mit der Anwendung auftreten.
- **Schutz vor Bedrohungen**. Dieser Bericht enthält Informationen über Ereignisse, die während der Ausführung der folgenden Komponenten der Anwendung 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 BadUSB-Angriffen
- 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 an:

1. Öffnen Sie das Hauptfenster der grafischen Oberfläche der Anwendung.
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.

   Im rechten Bereich des Fensters wird der Bericht mit einer Liste von Ereignissen angezeigt.

   Standardmäßig werden die Ereignisse in aufsteigender Reihenfolge der Werte in der Spalte **Datum** sortiert.
4. Wenn Sie ausführliche Informationen über ein Ereignis anzeigen möchten, wählen Sie das entsprechende Ereignis im Bericht aus.

   Am unteren Rand des Fensters wird ein Block angezeigt, der die Attribute dieses Ereignisses enthält.

Für eine zweckmäßige Verarbeitung von Berichten können Sie die auf dem Bildschirm gezeigten Daten folgendermaßen ändern:

- Filtern Sie die Liste der Ereignisse nach dem Zeitpunkt ihres Auftretens.
- Suchen Sie mithilfe der Suchfunktion nach einem bestimmten Ereignis.
- Zeigen Sie das ausgewählte Ereignis in einem separaten Abschnitt an.

Objekte im Backup anzeigen

In der grafischen Oberfläche können Sie die folgenden Aktionen für Objekte im Backup-Speicher ausführen:

- Informationen zu Objekten anzeigen, die im Backup auf dem Gerät abgelegt wurden.
- Objekte aus dem Backup in ihren ursprünglichen Verzeichnissen wiederherstellen.
- Objekte aus dem Backup löschen. Entfernte Objekte können später nicht wiederhergestellt werden.

Informationen über die Wiederherstellung und Löschung von Objekten im Ereignisprotokoll aufzeichnen.

So zeigen Sie die Objekte im Backup an:

1. Öffnen Sie das Hauptfenster der grafischen Oberfläche der Anwendung.
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.

Lizenzschlüssel verwalten

Über die grafische Oberfläche können Sie Lizenzschlüssel der Anwendung hinzufügen und entfernen sowie neben Informationen über die Lizenz, unter der die Anwendung verwendet wird, auch Informationen über die mit der Lizenz verknüpften Schlüssel anzeigen.

Um Kaspersky Endpoint Security auf einem geschützten Gerät zu aktivieren, müssen Sie der Anwendung einen Hauptlizenzschlüssel hinzufügen.

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

Wenn von der Hauptlizenz, unter der Sie die Anwendung verwenden, die erforderlichen zusätzlichen Funktionen von Kaspersky Endpoint Security nicht abgedeckt werden, müssen Sie der Anwendung auch einen Lizenzschlüssel für die zusätzlichen Funktionen hinzufügen:

- Einen separaten Lizenzschlüssel des Typs "Kaspersky Endpoint Detection and Response Optimum Add-on" (im Folgenden auch "EDR Optimum-Schlüssel" genannt), um die Komponente EDR-Optimum zu aktivieren.
- Einen separaten Lizenzschlüssel des Typs "Kaspersky Unified Monitoring and Analysis Platform Add-on" (im Folgenden auch "KUMA-Schlüssel" genannt), um die Funktionen der Kaspersky Unified Monitoring and Analysis Platform zu aktivieren.
- Einen separaten Lizenzschlüssel des Typs "Kaspersky Managed Detection and Response Optimum/Expert Add-on" (im Folgenden auch "MDR-Schlüssel" genannt), um die Funktionen der MDR-Komponente zu aktivieren.

Sie können der Anwendung auch einen Reserveschlüssel für die grundlegenden Funktionen und einen Reserveschlüssel für zusätzliche Funktionen hinzufügen. Der Reserveschlüssel wird aktiv, sobald die an den aktiven Schlüssel gebundene gültige Lizenz abläuft oder der aktive Schlüssel gelöscht wird. Ein Reserveschlüssel verhindert, dass nach Ablauf der Lizenz die Funktionalität der Anwendung eingeschränkt wird.

Ein Reserveschlüssel kann nur hinzugefügt werden, wenn bereits ein aktiver Lizenzschlüssel hinzugefügt wurde.

Einen Lizenzschlüssel hinzufügen

Wenn die Anwendung noch nicht aktiviert wurde (es wurde noch kein aktiver Haupt-Lizenzschlüssel hinzugefügt), können Sie die Anwendung mit einer kommerziellen Lizenz oder einer Testlizenz aktivieren.

So aktivieren Sie die Anwendung:

1. Öffnen Sie das Hauptfenster der grafischen Oberfläche der Anwendung.
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.

Das Fenster zeigt Informationen über den Schlüssel und die mit ihm verbundene Lizenz an.

b. Klicken Sie auf **Aktivieren**.

4. Wenn Sie die Anwendung mit einer Testlizenz aktivieren möchten, klicken Sie im Block **Testschlüssel** auf die Schaltfläche **Aktivieren**. Das Fenster zeigt Informationen über die Testlizenz und den zugehörigen Schlüssel an.

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

Nach der Aktivierung der Anwendung können Sie sowohl einen Reserveschlüssel für den aktiven Haupt-Lizenzschlüssel als auch bei Bedarf einen aktiven Schlüssel und einen Reserveschlüssel für zusätzliche Funktionen der Anwendung hinzufügen. Die Vorgehensweise zum Hinzufügen eines Reserveschlüssels für den Hauptschlüssel und zum Hinzufügen von Schlüsseln für zusätzliche Funktionen ist identisch.

So fügen Sie der Anwendungen einen Reserveschlüssels für den Hauptschlüssel oder Schlüssel für zusätzliche Funktionen hinzu:

1. Öffnen Sie das Hauptfenster der grafischen Oberfläche der Anwendung.

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.

   Das Fenster zeigt Informationen über den Schlüssel und die mit ihm verbundene Lizenz an.

4. Klicken Sie auf **Hinzufügen**.

Wenn Sie einen Haupt-Lizenzschlüssel hinzufügen und die Anwendung bereits aktiviert ist, wird der neue Schlüssel als Reserveschlüssel des Hauptschlüssels hinzugefügt.

Wenn Sie einen separaten Schlüssel für zusätzliche Funktionen hinzufügen, wird dieser als aktiver Schlüssel hinzugefügt, wenn der Anwendung nicht bereits zuvor ein Schlüssel für diese zusätzlichen Funktionen hinzugefügt wurde. Wenn der Anwendung bereits ein Schlüssel für diese zusätzlichen Funktionen hinzugefügt wurde, wird der neue Schlüssel als Reserveschlüssel der zusätzlichen Funktionen hinzugefügt.

Wenn der Anwendung bereits ein aktiver Schlüssel und ein Reserveschlüssel hinzugefügt wurden, ersetzt der neue Schlüssel den zuvor hinzugefügten Reserveschlüssel.

Der Schlüssel für eine Testlizenz und der Abonnementschlüssel können nicht als Reserveschlüssel hinzugefügt werden.

Einen Lizenzschlüssels entfernen

So entfernen Sie zur Anwendung hinzugefügten einen Lizenzschlüssel:

1. Öffnen Sie das Hauptfenster der grafischen Oberfläche der Anwendung.
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.
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.

Lizenz-Info anzeigen

So zeigen Sie Informationen zur Lizenz an:

1. Öffnen Sie das Hauptfenster der grafischen Oberfläche der Anwendung.
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 Block **Aktuelle Lizenzen** werden Informationen über die hinzugefügten aktiven Schlüssel (aktiver Hauptschlüssel und aktiver Schlüssel für zusätzliche Funktionen) und der mit ihnen verknüpften 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 Block **Reserveschlüssel** werden Informationen über die hinzugefügten Reserveschlüssel (Reserveschlüssel des Hauptschlüssels und Reserveschlüssel für zusätzliche Funktionen) und der mit ihnen verknüpften 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.

Temporären Zugriff auf ein Gerät erhalten

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 Oberfläche der Anwendung.
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 Oberfläche der Anwendung.
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**.

Informationen über die Anwendung anzeigen

Informationen zur installierten Anwendung und zum Gerät mit der installierten Anwendung können Sie im Fenster **Support** anzeigen. Diese wird durch Anklicken der Schaltfläche **Support** im unteren Bereich des Hauptfensters der grafischen Oberfläche der Anwendung geöffnet.

Im Fenster **Support** werden die folgenden Informationen angezeigt:

- Version der Anwendung
- **Lizenzschlüssel** – Aktiver Haupt-Lizenzschlüssel, welcher der Anwendung hinzugefügt wurde, oder Information über das Fehlen eines Schlüssels. Über den Link in diesem Feld können Sie das Fenster **Lizenz** öffnen, in dem detaillierte Informationen zur Lizenz angezeigt werden.
- **Schlüsselstatus** – Informationen über den Status des aktiven 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).

Im unteren Teil des Fensters **Support** werden die folgenden Links angezeigt:

- **Lizenzen**, der das Fenster **Lizenzen** öffnetn, welches detaillierte Informationen zur Lizenz anzeigt.
- **Wissensdatenbank**, der die Seite der Wissensdatenbank aufruft.
- **Support**, der die Seite von Kaspersky CompanyAccount aufruft.
- **Protokollierung**, der das Fenster der **Protokollierung** öffnet. In diesem Fenster können Sie Protokolldateien für die Anwendung erstellen und die Detailstufe der Protokolldateien konfigurieren.

  Um dem Link **Protokollierung** zu folgen, müssen Sie über Benutzerrechte mit Administratorrolle (admin) verfügen.

Protokolldatei erstellen

Sie können Protokolldateien der Anwendung erstellen und den Detailstufe der Protokolldateien über die grafische Benutzeroberfläche konfigurieren.

Für die Erstellung der Protokolldatei und die Konfiguration der Detailstufe sind Benutzerberechtigungen mit Administratorrolle (admin) erforderlich.

So erstellen Sie eine Protokolldatei:

1. Öffnen Sie das Hauptfenster der grafischen Oberfläche der Anwendung.
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 Level die **Stufe** der Protokolldatei.

   Sie sollten sich bei der Festlegung der erforderlichen Informationstiefe an die Empfehlung der Experten des Technischen Supports von Kaspersky halten. Standardmäßig beträgt der Wert **Diagnose (300)**.
5. Klicken Sie auf die Schaltfläche **Aktivieren**, um den Protokollierungsvorgang zu starten.
6. Reproduzieren Sie die Situation, in der das Problem auftritt.
7. Klicken Sie auf die Schaltfläche **Deaktivieren**, um den Protokollierungsvorgang zu beenden.

Die erstellten Protokolldateien werden im Verzeichnis /var/log/kaspersky/kesl/ gespeichert.

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. Der Name der Manifestdatei ist für jede Komponente gleich, der Inhalt der Manifestdateien ist jedoch unterschiedlich. Die Manifestdateien werden digital signiert. Auch ihre Integrität wird überprüft.

Um das Tool zur Integritätsprüfung auf Geräten mit Linux-Betriebssystemen auszuführen, ist ein Konto mit Root-Rechten erforderlich. Um das Tool zur Integritätsprüfung auf Geräten mit Windows-Betriebssystemen auszuführen, ist ein Konto mit Administrator-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 für die 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 das Verzeichnis des Web-Plug-ins zur Verwaltung von Kaspersky Endpoint Security zu überprüfen:
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console\server\plugins\kesl_Versionsnummer\integrity_check.xml – für Windows-Geräte
  - /var/opt/kaspersky/ksc-web-console/server/plugins/kesl_<Versionsnummer>/integrity_check.xml – für Linux-Geräte

Um die Integrität einer Komponente der Lösung zu überprüfen, müssen Sie das Tool im Speicherordner des Tools für diese Komponente ausführen.

Um das Tool zur Integritätsprüfung starten, führen Sie einen der folgenden Befehle aus:

- Um die Integrität des Anwendungspakets zu überprüfen:

  ```
  integrity_checker [<Pfad zur Manifestdatei>] --crl
  /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-with-filename
  ```

- Um die Integrität des Pakets für die grafische Benutzeroberfläche zu überprüfen:

  ```
  integrity_checker <Pfad zur Manifestdatei> --crl
  /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-with-filename
  ```

- Für die Integritätsprüfung des MMC-Plug-ins für die Verwaltung von Kaspersky Endpoint Security:

  ```
  integrity_checker.exe [<Pfad zur Manifestdatei>]
  ```

- Um die Integrität des Administrationsagenten zu überprüfen:

  ```
  integrity_checker <Pfad zur Manifestdatei>
  ```

- Um die Integrität des Verzeichnisses des Web-Plug-ins zur Verwaltung von Kaspersky Endpoint Security zu überprüfen:

  ```
  integrity_checker <Pfad zur Manifestdatei> --crl
  /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds
  ```

Standardmäßig wird der Pfad zum Manifest verwendet, die sich in dem Verzeichnis befindet, in dem das Tool zur Integritätsprüfung ausgeführt wird.

Das Tool kann mit den folgenden optionalen Einstellungen ausgeführt werden:

- `--crl <Verzeichnis>` 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 <Dateiname>`, wobei `<Dateiname>` der Name der Datei ist, in der Ereignisse mit der Informationstiefe DEBUG aufgezeichnet werden, die während der Untersuchung aufgetreten sind.
- `--signature-type kds` ist der zu überprüfende Signaturtyp (diese Option ist für die Untersuchung des Verzeichnisses des Web-Plug-ins zur Verwaltung von Kaspersky Endpoint Security erforderlich).
- `--signature-type kds-with-filename` – Typ der zu prüfenden Signatur (dieser Parameter ist obligatorisch für die Überprüfung des Anwendungspakets und des Pakets für die grafische Benutzeroberfläche).
- `--single-file <Datei>` 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.

Eine Beschreibung aller verfügbaren Einstellungen des Tools zur Integritätsprüfung finden Sie in der Hilfe zu den Einstellungen des Tools, die Sie mithilfe des Befehls `integrity_checker --help` aufrufen.

Das Ergebnis der Überprüfung der Manifestdatei wird wie folgt angezeigt:

- `SUCCEEDED` – Die Integrität der Dateien wurde bestätigt (Rückgabecode 0).
- `FAILED` – Die Integrität der Dateien konnte nicht bestätigt werden (Rückgabecode ist nicht 0).

Wenn 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.

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 während des gesamten Lebenszyklus von Kaspersky Endpoint Security (siehe die Seite zum Lebenszyklus von Anwendungen). Bitte machen Sie sich mit den Support-Richtlinien vertraut, bevor Sie sich an den Technischen Support wenden.

Eine Kontaktaufnahme mit den Support-Experten ist auf folgende Weise möglich:

- Aufrufen der Webseite des Technische Supports
- Anfrage an den Technischen Support von Kaspersky über das Portal Kaspersky CompanyAccount.

Technischer Support über das Kaspersky CompanyAccount

Kaspersky CompanyAccount – Ein Webdienst für Unternehmen, die Anwendungen von Kaspersky verwenden. Das Portal Kaspersky CompanyAccount dient der Kontaktaufnahme mit den Spezialisten von Kaspersky über elektronische Anfragen. Im Portal Kaspersky CompanyAccount können Sie den Status der Bearbeitung von E-Mail-Anfragen durch die Kaspersky-Experten verfolgen und die Chronik der E-Mail-Anfragen speichern.

Sie können alle Mitarbeiter Ihrer Organisation im Rahmen eines Benutzerkontos für Kaspersky CompanyAccount registrieren. Mithilfe eines Benutzerkontos können Sie die elektronischen Anfragen der registrierten Mitarbeiter an Kaspersky zentral kontrollieren, sowie die Berechtigungen dieser Mitarbeiter für Kaspersky CompanyAccount verwalten.

Das Portal Kaspersky CompanyAccount ist in den folgenden Sprachen verfügbar:

- Deutsch
- Spanisch
- Italienisch
- Deutsch
- Polnisch
- Portugiesisch
- Russisch
- Französisch
- Japanisch

Weitere Informationen zu Kaspersky CompanyAccount erhalten Sie auf der Website des Technischen Supports.

Informationen für den Technischen Support abrufen

Nachdem Sie die Spezialisten des Technischen Supports von Kaspersky über ein Problem informiert haben, werden Sie möglicherweise aufgefordert, *eine 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 Anwendung oder in den Anleitungen der Support-Experten beschrieben, so kann die Anwendung oder das Betriebssystem verlangsamt oder beeinträchtigt werden, das Schutzniveau sinken und der Zugriff auf und die Integrität von Informationen beschädigt werden.

Über Protokolldateien der Anwendung

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 der Anwendung aktivieren oder deaktivieren und den Detaillierungsgrad der Protokolldateien in der Befehlszeile mithilfe der allgemeinen Anwendungseinstellungen sowie der grafischen Benutzeroberfläche konfigurieren.

Wenn Sie die Erstellung von Protokolldateien der Anwendung aktiviert haben, werden die Protokolldateien standardmäßig im Verzeichnis /var/log/kaspersky/kesl/ gespeichert. Für den Zugriff auf dieses Verzeichnis sind Root-Rechte erforderlich.

Das Speichern der Protokolldateien der Anwendung erfordert zusätzlichen Speicherplatz, der über den in den Mindestanforderungen an die Hardware angegebenen Speicherplatz hinausgeht.

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.

Inhalt von Protokolldateien der Anwendung

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.

Protokolleinstellungen der Anwendung konfigurieren

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.

Wenn Sie die Anwendung über die Befehlszeile verwalten, können Sie die Einstellungen für die Protokollierung der Anwendung in den allgemeinen Anwendungseinstellungen konfigurieren.

Konfiguration der Protokollierung in der Web Console

In der Web Console können Sie Einstellungen für die Programmablaufverfolgung in den Richtlinieneigenschaften verwalten (**Programmeinstellungen** → **Allgemeine Einstellungen** → **Technischer Support**).

Sie müssen die App neu starten, um die Einstellungen für die Ablaufverfolgung der App anzuwenden.

Konfiguration der Protokollierung in der Verwaltungskonsole

In der Verwaltungskonsole können Sie die Einstellungen für die Programmablaufverfolgung in den Richtlinieneigenschaften verwalten (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Sicherheitskontrolle** → **Programmeinstellungen**).

Wenn Sie im Block **Protokollierungs- und Dump-Einstellungen** auf den Link **Konfigurieren** klicken, öffnet sich ein Fenster, in dem Sie Einstellungen der Protokollierung konfigurieren können (siehe untere Tabelle).

Parameter für die Ablaufverfolgung der App

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 zum Speichern von 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.

Sie müssen die App neu starten, um die Einstellungen für die Ablaufverfolgung der App anzuwenden.

Konfiguration der Protokollierung über die Befehlszeile

Über die Befehlszeile können Sie die Einstellungen für Protokollierung der Anwendung in den allgemeinen Anwendungseinstellungen mithilfe der Parameter `TraceLevel`, `TraceFolder`, `TraceMaxFileCount` und `TraceMaxFileSize` konfigurieren.

Mit dem Parameter `TraceLevel` können Sie die Erstellung von Protokolldateien für die Anwendung aktivieren oder deaktivieren und die Detailstufe innerhalb der Protokolldateien angeben. Der Parameter kann die folgenden Werte annehmen:

- `Detailed` – detaillierteste Protokolldateien erstellen.
- `MediumDetailed` – Protokolldatei mit Info- und Fehlermeldungen erstellen
- `NotDetailed` – Protokolldatei mit Fehlermeldungen erstellen
- `None` (Standardwert) – Keine Protokolldatei erstellen.

Mit dem Parameter `TraceFolder` können Sie das Verzeichnis angeben, in dem die Protokolldateien der Anwendung gespeichert werden. Standardwert: /var/log/kaspersky/kesl. Wenn Sie ein anderes Verzeichnis angeben, stellen Sie sicher, dass das ausschließlich das Benutzerkonto, unter dem Kaspersky Endpoint Security ausgeführt wird, eine Lese- und Schreibberechtigung für dieses Verzeichnis besitzt (Berechtigung rwx------ 700). Für den Zugriff auf das Standardverzeichnis zum Speichern von Protokolldateien sind Root-Rechte erforderlich.

Mit dem Parameter `TraceMaxFileCount` können Sie die maximale Anzahl der Protokolldateien für die Anwendung angeben. Der Parameter kann die Werte 1 bis 10000 annehmen. Standardwert: 10.

Mit dem Parameter `TraceMaxFileSize` können Sie die maximale Größe der Protokolldateien für die Anwendung angeben (in MB). Der Parameter kann die Werte 1 bis 1000 annehmen. Standardwert: 500.

Sie können den Wert von Parametern mithilfe von Befehlszeilenparametern oder mithilfe einer Konfigurationsdatei ändern, die alle allgemeinen Anwendungseinstellungen enthält.

Nach dem Ändern der Werte für die Parameter `TraceFolder`, `TraceMaxFileCount` und `TraceMaxFileSize` müssen Sie die Anwendung neu starten.

Über Protokolldateien der Verwaltungs-Plug-ins für die Anwendung

Es werden keine Protokolldateien der Verwaltungs-Plug-ins automatisch an Kaspersky gesendet.

Protokolldateien werden in lesbarer Form gespeichert. Es wird empfohlen, die Informationen bis zu ihrer Übermittlung an Kaspersky vor unbefugtem Zugriff zu schützen.

Protokolldateien des MMC-Verwaltungs-Plug-ins

Wenn Sie zur Verwaltung von Kaspersky Endpoint Security die Verwaltungskonsole verwenden, können Informationen über Ereignisse während der Ausführung des MMC-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

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 im Installationsassistenten von Web Console die Protokollierung im Aktivitätsprotokoll von Web Console aktiviert ist (weitere Informationen dazu finden Sie in der Hilfe von Kaspersky Security Center).

Die Protokolldateien des Web-Plug-ins werden im Installationsordner der Web Console im Unterordner "logs" gespeichert.

Inhalt der Protokolldateien der Verwaltungs-Plug-ins

Die Protokolldateien enthalten die folgenden allgemeinen Informationen:

- 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 die folgenden Informationen enthalten:

- Personenbezogene Daten, einschließlich Nachname, Vorname und Vatersname, wenn diese Daten Teil des Pfads zu den Dateien sind.
- Der Kontoname zur Anmeldung am Betriebssystem, wenn der Kontoname Teil des Dateinamens ist.

Über Dump-Dateien

Eine *Dump-Datei* enthält alle Informationen zum Arbeitsspeicher der Prozesse von Kaspersky Endpoint Security zum Zeitpunkt der Erstellung der Dump-Datei.

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 Erstellung einer Dump-Datei im Falle eines Absturzes der Anwendung aktivieren oder deaktivieren.

Wenn Sie die Erstellung von Dump-Dateien aktiviert haben, werden die Dump-Dateien standardmäßig in 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. Für die Dump-Dateien des kesl-Prozesses können Sie ein anderes Speicherverzeichnis angeben. Wenn Sie ein anderes Verzeichnis angeben, stellen Sie sicher, dass nur root Lese- und Schreibberechtigungen für dieses Verzeichnis hat (Berechtigungen `700` oder `rwx--------`).

Das Speichern der Dump-Dateien der Anwendung erfordert zusätzlichen Speicherplatz, der über den in den Mindestanforderungen an die Hardware angegebenen Speicherplatz hinausgeht.

Dump-Dateien werden auf dem Gerät gespeichert, solange die Anwendung verwendet wird. Bei der Deinstallation der Anwendung werden sie dauerhaft gelöscht. Es werden keine Dump-Dateien automatisch an Kaspersky gesendet.

Parameter der Dump-Erstellung konfigurieren

Wenn Sie Kaspersky Endpoint Security über Kaspersky Security Center verwalten, können Sie die Einstellungen für die Dump-Erstellung in den Einstellungen der Richtlinie von Kaspersky Endpoint Security entweder über die Web Console oder die Verwaltungskonsole konfigurieren.

Wenn Sie die Anwendung über die Befehlszeile verwalten, können Sie die Dump-Erstellung mithilfe der Konfigurationsdatei kesl.ini aktivieren oder deaktivieren.

Die maximale Anzahl von Dump-Dateien ist begrenzt.

In Abhängigkeit von den Betriebssystem-Einstellungen werden möglicherweise keine benutzerdefinierten Dump-Dateien erstellt. Stellen Sie sicher, dass das folgende Parameter-Wert-Paar angegeben ist: `sysctl kernel.yama.ptrace_scope=0`.

Konfiguration der Dump-Erstellung in der Web Console

In der Web Console können Sie die Einstellungen für die Programm-Dump-Datei in den Richtlinieneigenschaften verwalten (**Programmeinstellungen** → **Allgemeine Einstellungen** → **Technischer Support**).

Die Parameter zur Dump-Erstellung in den Richtlinieneigenschaften der Web Console werden in Anhang 5 beschrieben.

Sie müssen die Anwendung neu starten, um die Einstellungen zum Erstellen eines Dumps anzuwenden.

Konfiguration der Dump-Erstellung in der Verwaltungskonsole

In der Verwaltungskonsole können Sie die Einstellungen für das Erstellen von Dump-Dateien der App in den Richtlinieneigenschaften verwalten (Richtlinien in der Verwaltungskonsole verwalten, Erstellen einer Richtlinie mithilfe der Verwaltungskonsole) (**Sicherheitskontrolle** → **Programmeinstellungen**).

Klicken Sie unter **Trace- und Dump-Einstellungen** auf **Konfigurieren**, um ein Fenster zu öffnen, in dem Sie die Einstellungen für das Erstellen von Dump-Dateien bearbeiten können (siehe Tabelle unten).

Einstellungen der Dump-Erstellung

Parameter	Description
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.

Sie müssen die Anwendung neu starten, um die Einstellungen zum Erstellen eines Dumps anzuwenden.

Konfiguration der Dump-Erstellung in der Befehlszeile

So konfigurieren Sie die Dump-Erstellung mithilfe der Konfigurationsdatei kesl.ini:

1. Beenden Sie Kaspersky Endpoint Security.
2. Öffnen Sie die Datei /var/opt/kaspersky/kesl/common/kesl.ini zur Bearbeitung.
3. Legen Sie im Abschnitt **[General]** den Parameterwert fest:
   - `CoreDumps=yes` – Dump-Erstellung im Falle eines Absturzes der Anwendung aktivieren.
   - `CoreDumps=no` – Dump-Erstellung deaktivieren.
4. Wenn Sie das Standardverzeichnis ändern möchten, in dem Dump-Dateien gespeichert werden, geben Sie den Verzeichnispfad im Parameter `CoreDumpsPath` an.
5. Starten Sie Kaspersky Endpoint Security.

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. Befehle zur Verwaltung von Kaspersky Endpoint Security

Kaspersky Endpoint Security wird über die Befehlszeile mithilfe der Verwaltungsbefehle für Kaspersky Endpoint Security verwaltet.

Sie können die Hilfe zu Verwaltungsbefehlen mit dem folgenden Befehl anzeigen:

```
kesl-control --help <Präfix der Befehlsgruppe>
```

dabei kann `<Präfix der Befehlsgruppe>` die folgenden Werte annehmen:

- -A – Befehle zur Verwaltung der Programmkontrolle
- -B – Befehle zur Backup-Verwaltung
- -C: Befehle zur Verwaltung der allgemeinen Einstellungen für die Untersuchung von Containern (Untersuchung von Containern, Container-Überwachung)
- -D – Befehle zur Verwaltung der Gerätekontrolle
- -E: Befehle zur Verwaltung von Programmereignissen (Ereignisse über die Befehlszeile anzeigen, Ereignisse in Kaspersky Security Center anzeigen)
- -F – Befehle zur Firewall-Verwaltung
- -H – Befehle zur Verwaltung blockierter Geräte
- -J – Befehle zur Verwaltung der Sammlung von Kennzahlen zum Systemzustand
- -L – Befehle zur Verwaltung der Lizenzschlüssel
- -M – Befehle zur Verwaltung der Integrationsparameter der Anwendung Kaspersky Endpoint Security mit Kaspersky Unified Monitoring and Analysis Platform
- -N – Befehle zur Verwaltung der Einstellungen für die Untersuchung des Netzwerkverkehrs
- -Q – Befehle zur Verwaltung der Quarantäne
- -R – Befehle zur Verwaltung der Integrationsparameter der Anwendung Kaspersky Endpoint Security mit Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), Kaspersky Endpoint Detection and Response Expert (on-premise) und Kaspersky Endpoint Detection and Response Optimum.
- -S – Befehle der Statistik

- -T – Befehle zur Verwaltung der Aufgaben und Einstellungen der Anwendung
- -U – Befehle zur Verwaltung von Benutzern und Benutzerrollen
- -V – Befehle der Anwendung im Light Agent-Modus zum Schutz virtueller Umgebungen
- -W: Befehle zur Ereignisausgabe (Ereignisse über die Befehlszeile anzeigen, Ereignisse in Kaspersky Security Center anzeigen)
- -X – Befehle zur Verwaltung der Integrationsparameter der Anwendung Kaspersky Endpoint Security mit der Komponente Sandbox

Befehle zur Verwaltung der Einstellungen und Aufgaben der App

Das Präfix -T gibt an, dass der Befehl zur Gruppe der Befehle zur Verwaltung von Programmeinstellungen und Aufgaben gehört.

Das Präfix -C gibt an, dass der Befehl zur Gruppe der Befehle zur Verwaltung der Einstellungen für die Untersuchung von Containern (Untersuchung von Containern, Container-Überwachung) 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.

Befehlssyntax

```
kesl-control [-T] --export-settings [--file <Pfad der Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, in der die Anwendungseinstellungen gespeichert werden.

`--json` wird angegeben, um die Einstellungen im JSON-Format auszugeben. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Befehl kesl-control --import-settings

Mit diesem Befehl können Sie alle 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).

Befehlssyntax

```
kesl-control [-T] --import-settings --file <Pfad der Konfigurationsdatei> [--json]
```

Argumente und Schlüssel

`--file <Pfad zur Konfigurationsdatei>` ist der vollständige Pfad zur Konfigurationsdatei, aus der die Einstellungen in das Programm importiert 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 --update-application

Mit diesem Befehl können Sie das heruntergeladene Update der Anwendungsmodule installieren.

> Befehl kann nicht ausgeführt werden, wenn die Anwendung im Light Agent-Modus ausgeführt wird.

Befehlssyntax

```
kesl-control [-T] --update-application
```

Befehle zur Verwaltung der allgemeinen Anwendungseinstellungen

Befehl kesl-control --get-app-settings

Mit diesem Befehl können Sie die aktuellen Werte der allgemeinen Anwendungseinstellungen in die Konsole oder in eine Konfigurationsdatei ausgeben.

Befehlssyntax

```
kesl-control [-T] --get-app-settings [--file <Pfad zur Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`--file <Pfad der Konfigurationsdatei>` – Pfad der Konfigurationsdatei, in der die allgemeinen Anwendungseinstellungen ausgegeben werden. Wenn Sie den Schalter `--file` nicht angeben, werden die Einstellungen in die Konsole ausgegeben.

Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.

`--json` wird angegeben, um die Einstellungen im JSON-Format auszugeben. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Befehl kesl-control --set-app-settings

Mit diesem Befehl können Sie die Werte der allgemeinen Anwendungseinstellungen mithilfe von Befehlsschaltern oder durch Importieren von Einstellungen aus einer angegebenen Konfigurationsdatei festlegen.

Befehlssyntax

So legen Sie Einstellungen mithilfe von Befehlsschaltern fest:

```
kesl-control [-T] --set-app-settings <Name der Einstellung>=<Wert der Einstellung>
[<Name der Einstellung>=<Wert der Einstellung>]
```

So legen Sie Einstellungen mithilfe einer Konfigurationsdatei fest:

```
kesl-control [-T] --set-app-settings --file <Pfad zur Konfigurationsdatei> [--json]
```

Argumente und Schlüssel

`<Name der Einstellung>=<Wert der Einstellung>` ist der Name und der Wert einer der allgemeinen Programmeinstellungen.

`--file <Pfad zur Konfigurationsdatei>` ist der vollständige Pfad zur Konfigurationsdatei, aus der die Einstellungen in das Programm importiert werden.

`--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.

Befehlssyntax

```
kesl-control [-T] --get-settings <ID/Name der Aufgabe> [--file <Pfad der
Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`--file <Pfad der Konfigurationsdatei>` ist der Pfad zur Konfigurationsdatei, in die die Aufgabeneinstellungen geschrieben werden. Wenn Sie den Schalter `--file` nicht angeben, werden die Einstellungen in die Konsole ausgegeben.

Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.

`--json` wird angegeben, um die Einstellungen im JSON-Format auszugeben. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Befehl kesl-control --set-settings

Mit diesem Befehl können Sie die Werte der Einstellungen der angegebenen Aufgabe mithilfe von Befehlsschaltern oder durch Importieren von Einstellungen aus einer angegebenen Konfigurationsdatei festlegen.

Befehlssyntax

So legen Sie Einstellungen mithilfe von Befehlsschaltern fest:

```
kesl-control [-T] --set-settings <ID/Name der Aufgabe> <Name der Einstellung>=<Wert der Einstellung> [<Name der Einstellung>=<Wert der Einstellung>] [--add-path <Pfad>] [--del-path <Pfad>] [--add-exclusion <Pfad>] [--del-exclusion <Pfad>]
```

So legen Sie Einstellungen mithilfe einer Konfigurationsdatei fest:

```
kesl-control [-T] --set-settings <ID/Name der Aufgabe> --file <Pfad der Konfigurationsdatei> [--json]
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`<Name der Einstellung>=<Wert der Einstellung>` – Name und Wert einer der Aufgabeneinstellungen.

`--add-path <Pfad>` fügt einen Pfad zu einem Verzeichnis mit zu untersuchenden Objekten hinzu.

`--del-path <Pfad>` entfernt einen Pfad zu einem Verzeichnis mit zu untersuchenden Objekten.

`--add-exclusion <Pfad>` fügt einen Pfad zu einem Verzeichnis mit Objekten hinzu, die von der Untersuchung ausgeschlossen werden sollen.

`--del-exclusion <Pfad>` entfernt einen Pfad zu einem Verzeichnis mit Objekten, die von der Untersuchung ausgeschlossen werden sollen.

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die Einstellungen der Aufgabe importiert 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 --set-to-default

Mit diesem Befehl können Sie die Standardwerte der Einstellungen der angegebenen Aufgabe wiederherstellen.

Befehlssyntax

```
kesl-control [-T] --set-settings <ID/Name der Aufgabe> --set-to-default
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Befehl kesl-control --get-schedule

Mit diesem Befehl können Sie den aktuellen Zeitplan für den Start der angegebenen Aufgabe in die Konsole oder in eine Konfigurationsdatei ausgeben.

Befehlssyntax

```
kesl-control [-T] --get-schedule <ID/Name der Aufgabe> [--file <Pfad der
Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`--file <Pfad der Konfigurationsdatei>` ist der Pfad zur Konfigurationsdatei, in die die Einstellungen des Aufgabenzeitplans geschrieben werden. Wenn Sie den Schalter `--file` nicht angeben, werden die Einstellungen in die Konsole ausgegeben.

Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.

`--json` wird angegeben, um die Einstellungen im JSON-Format auszugeben. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Befehl kesl-control --set-schedule

Mit diesem Befehl können Sie den Zeitplan der angegebenen Aufgabe mithilfe von Befehlsschaltern oder durch Importieren von Einstellungen aus einer angegebenen Konfigurationsdatei festlegen.

Befehlssyntax

So legen Sie Einstellungen mithilfe von Befehlsschaltern fest:

```
kesl-control [-T] --set-schedule <ID/Name der Aufgabe> <Name der Einstellung>=<Wert der Einstellung> [<Name der Einstellung>=<Wert der Einstellung>]
```

So legen Sie Einstellungen mithilfe einer Konfigurationsdatei fest:

```
kesl-control [-T] --set-schedule <ID/Name der Aufgabe> --file <Pfad der Konfigurationsdatei> [--json]
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`<Name der Einstellung>=<Wert der Einstellung>` ist der Name und der Wert einer der Einstellungen des Aufgabenzeitplans.

`--file <Pfad der Konfigurationsdatei>` – Vollständiger Pfad der Konfigurationsdatei, aus der die Einstellungen des Aufgabenzeitplans importiert 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.

Befehle zur Aufgabenverwaltung

Befehl kesl-control --get-task-list

Mit diesem Befehl können Sie die Liste der vorhandenen Anwendungsaufgaben anzeigen.

Befehlssyntax

```
kesl-control [-T] --get-task-list [--json]
```

Argumente und Schlüssel

`--json` – Gibt die Einstellungen im JSON-Format aus.

Befehl kesl-control --get-task-state

Mit diesem Befehl können Sie den Status der angegebenen Aufgabe ausgeben.

Befehlssyntax

```
kesl-control [-T] --get-task-state <ID/Name der Aufgabe> [--json]
```

Argumente und Schlüssel

< ID/Name der Aufgabe > – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

--json – Gibt die Einstellungen im JSON-Format aus.

Befehl kesl-control --create-task

Mit diesem Befehl können Sie eine Aufgabe des angegebenen Typs mit Standardeinstellungen oder mit den in der Konfigurationsdatei angegebenen Einstellungen erstellen.

Befehlssyntax

So erstellen Sie eine Aufgabe mit Standardeinstellungen:

```
kesl-control [-T] --create-task < Aufgabenname > --type < Aufgabentyp >
```

So erstellen Sie eine Aufgabe mit Einstellungen aus der Konfigurationsdatei:

```
kesl-control [-T] --create-task < Aufgabenname > --type < Aufgabentyp > [--file < Pfad zur Konfigurationsdatei >] [--json]
```

Argumente und Schlüssel

< Aufgabenname > – Name, den Sie für eine neue Aufgabe vergeben.

< Aufgabentyp > ist die Bezeichnung für den Typ der Aufgabe, die Sie erstellen.

--file < Pfad zur Konfigurationsdatei > 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

Mit diesem Befehl können Sie eine Aufgabe löschen.

Befehlssyntax

```
kesl-control [-T] --delete-task < ID/Name der Aufgabe >
```

Argumente und Schlüssel

< ID/Name der Aufgabe > – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Befehl kesl-control --start-task

Mit diesem Befehl können Sie eine Aufgabe starten.

Befehlssyntax

```
kesl-control [-T] --start-task <ID/Name der Aufgabe> [-W] [--progress]
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`[-W]` – Ausgabe aktueller Ereignisse aktivieren.

`[--progress]` – Fortschritt der laufenden Aufgabe anzeigen.

Befehl kesl-control --stop-task

Mit diesem Befehl können Sie die Aufgabe beenden.

Befehlssyntax

```
kesl-control [-T] --stop-task <ID/Name der Aufgabe> [-W]
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

`[-W]` – Ausgabe aktueller Ereignisse aktivieren.

Befehl kesl-control --suspend-task

Mit diesem Befehl können Sie eine Aufgabe anhalten.

Befehlssyntax

```
kesl-control [-T] --suspend-task <ID/Name der Aufgabe>
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Befehl kesl-control --resume-task

Mit diesem Befehl können Sie die Ausführung der Aufgabe fortsetzen.

Befehlssyntax

```
kesl-control [-T] --resume-task <ID/Name der Aufgabe>
```

Argumente und Schlüssel

`<ID/Name der Aufgabe>` – ID, die der Aufgabe zum Zeitpunkt der Erstellung zugewiesen wurde, oder der Name der Aufgabe in der Befehlszeile.

Befehl kesl-control --scan-file

Mit diesem Befehl können Sie eine Aufgabe zur benutzerdefinierten Untersuchung erstellen und starten.

Befehlssyntax

```
kesl-control [-T] --scan-file <Pfad> [--action <Aktion>]
```

Argumente und Schlüssel

`<Pfad>` – Pfad zu der Datei oder dem Verzeichnis, das Sie überprüfen möchten. Sie können mehrere, durch Leerzeichen getrennte Pfade angeben.

`--action <Aktion>` – Aktion, welche die Anwendung 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.

Befehlssyntax

```
kesl-control [-T] --scan-container <ID/Name[:Tag]>
```

Argumente und Schlüssel

`<ID/Name[:Tag]>` – Name oder ID des Containers oder Images. Bei der Untersuchung mehrerer Objekte können **Masken** verwendet werden.

Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen.

Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`.

Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`.

Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt.

Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Befehle zur Verwaltung der Ausführungsprävention für Objekte

Befehl kesl-control --get-prevention-state

Der Befehl gibt in der Konsole die Regeln der Ausführungsprävention für Objekte für die angegebene Komponente aus.

Befehlssyntax

```
kesl-control [-T] --get-prevention-state [--kata|--edro]
```

Argumente und Schlüssel

`--kata` – Regeln der Ausführungsprävention für Objekte aus EDR Expert (on-premise).

`--edro` – Regeln der Ausführungsprävention für Objekte aus EDR Optimum.

Befehle zur Verwaltung der allgemeinen Einstellungen für die Untersuchung von Containern

Befehl kesl-control --get-container-settings

Mit diesem Befehl können Sie die aktuellen Werte der allgemeinen Einstellungen für die Untersuchung von Containern in die Konsole oder in eine Konfigurationsdatei ausgeben.

Befehlssyntax

```
kesl-control [-C] --get-container-settings [--file <Pfad der Konfigurationsdatei>] [--
json]
```

Argumente und Schlüssel

`--file <Pfad der Konfigurationsdatei>` ist der Pfad der Konfigurationsdatei, in die die allgemeinen Einstellungen der Untersuchung von Containern geschrieben werden. Wenn Sie den Schalter `--file` nicht angeben, werden die Einstellungen in die Konsole ausgegeben.

Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.

`--json` wird angegeben, um die Einstellungen im JSON-Format auszugeben. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Befehl kesl-control --set-container-settings

Mit diesem Befehl können Sie die Werte der allgemeinen Einstellungen für die Untersuchung von Containern mithilfe von Befehlsschaltern oder durch Importieren von Einstellungen aus einer angegebenen Konfigurationsdatei festlegen.

Befehlssyntax

So legen Sie Einstellungen mithilfe von Befehlsschaltern fest:

```
kesl-control [-C] --set-container-settings <Name der Einstellung>=<Wert der Einstellung>
[<Name der Einstellung>=<Wert der Einstellung>]
```

So legen Sie Einstellungen mithilfe einer Konfigurationsdatei fest:

```
kesl-control [-C] --set-container-settings --file <Pfad der Konfigurationsdatei> [--
json]
```

Argumente und Schlüssel

`<Name der Einstellung>=<Wert der Einstellung>` ist der Name und der Wert einer der allgemeinen Einstellungen der Untersuchung von Containern.

`--file <Pfad der Konfigurationsdatei>` ist der vollständige Pfad der Konfigurationsdatei; die allgemeinen Einstellungen der Untersuchung von Containern aus dieser Datei werden in die App importiert.

`--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.

Befehlssyntax

```
kesl-control -N --query user

kesl-control -N --query auto

kesl-control -N --query kl
```

Befehl kesl-control --clear-web-auto-excluded

Mit diesem Befehl können Sie die Liste der Domänen löschen, welche die Anwendung automatisch von der Untersuchung ausgeschlossen hat.

Befehlssyntax

```
kesl-control -N --clear-web-auto-excluded
```

Befehl kesl-control --get-net-settings

Mit diesem Befehl können Sie die aktuellen Werte der Einstellungen für die Untersuchung des Netzwerkverkehrs in die Konsole oder in eine Konfigurationsdatei ausgeben.

Befehlssyntax

```
kesl-control [-N] --get-net-settings [--file <Pfad der Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`--file <Pfad der Konfigurationsdatei>` ist der Pfad der Konfigurationsdatei, in die die Einstellungen für die Untersuchung des Netzwerkverkehrs geschrieben werden. Wenn Sie den Schalter `--file` nicht angeben, werden die Einstellungen in die Konsole ausgegeben.

Wenn Sie den Dateinamen ohne Pfad eingeben, wird die Datei im aktuellen Verzeichnis erstellt. Wenn die Datei unter dem angegebenen Pfad vorhanden ist, wird sie überschrieben. Wenn das angegebene Verzeichnis nicht existiert, wird die Konfigurationsdatei nicht erstellt.

`--json` wird angegeben, um die Einstellungen im JSON-Format auszugeben. Wenn Sie den Schalter `--json` nicht angeben, werden die Einstellungen im INI-Format ausgegeben.

Befehl kesl-control --set-net-settings

Mit diesem Befehl können Sie die Werte der Einstellungen für die Untersuchung des Netzwerkverkehrs mithilfe von Befehlsschaltern oder durch Importieren von Einstellungen aus einer angegebenen Konfigurationsdatei festlegen.

Befehlssyntax

So legen Sie Einstellungen mithilfe von Befehlsschaltern fest:

```
kesl-control [-N] --set-net-settings <Name der Einstellung>=<Wert der Einstellung>
[<Name der Einstellung>=<Wert der Einstellung>]
```

So legen Sie Einstellungen mithilfe einer Konfigurationsdatei fest:

```
kesl-control [-N] --set-net-settings --file <Pfad der Konfigurationsdatei> [--json]
```

Argumente und Schlüssel

`<Name der Einstellung>=<Wert der Einstellung>` ist der Name und der Wert einer der Einstellungen für die Untersuchung des Netzwerkverkehrs.

`--file <Pfad der Konfigurationsdatei>` ist der vollständige Pfad der Konfigurationsdatei, aus der die Einstellungen für die Untersuchung des Netzwerkverkehrs importiert werden.

`--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.

Befehl kesl-control --list-certificates

Mit diesem Befehl können Sie die Liste vertrauenswürdiger Stammzertifikate ausgeben.

Befehlssyntax

```
kesl-control [-N] --list-certificates
```

Befehl kesl-control --add-certificate

Mit dem Befehl können der Liste mit vertrauenswürdigen Stammzertifikaten ein Zertifikat hinzufügen.

Befehlssyntax

```
kesl-control [-N] --add-certificate <Pfad des Zertifikats>
```

Argumente und Schlüssel

`< Pfad des Zertifikats >` – Pfad der Zertifikatsdatei, die Sie hinzufügen möchten, im PEM- oder DER-Format.

Befehl kesl-control --remove-certificate

Mit diesem Befehl können Sie ein Zertifikat aus der Liste der vertrauenswürdigen Stammzertifikate entfernen.

Befehlssyntax

```
kesl-control [-N] --remove-certificate < Antragsteller des Zertifikats >
```

Befehl kesl-control --add-bypass-endpoints

Mit dem Befehl können Sie dem Abfangen des Datenverkehrs eine Ausnahme hinzufügen.

Befehlssyntax

```
kesl-control [-N] --add-bypass-endpoints --direction <in|out> --remote-ip < Remote-IP-Adresse > --dst-port < Zielport >
```

Argumente und Schlüssel

`<in|out>` – Richtung des Datenverkehrs der ausgeschlossenen Verbindung: eingehend oder ausgehend.

`< Remote-IP-Adresse >` – Adresse des Remote-Geräts im IPv4- oder IPv6-Format. 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.

`< Zielport >` – Port auf dem geschützten Gerät (bei Ausschluss eingehenden Datenverkehrs) oder Port auf dem Remote-Gerät (bei Ausschluss ausgehenden Datenverkehrs). 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.

Befehlssyntax

```
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.

Befehlssyntax

```
kesl-control [-N] --remove-bypass-endpoints --direction <in|out> --remote-ip <Remote-IP-Adresse> --dst-port <Ziel-Port>
```

Argumente und Schlüssel

`<in|out>` – Richtung des Datenverkehrs der ausgeschlossenen Verbindung: eingehend oder ausgehend.

`< Remote-IP-Adresse >` – Adresse des Remote-Geräts im IPv4- oder IPv6-Format, deren Datenverkehr (abhängig von der Richtung des Datenverkehrs) vom Abfangen ausgeschlossen ist.

`< Zielport >` – Port auf dem geschützten Gerät (bei Ausschluss eingehenden Datenverkehrs) oder Port auf dem Remote-Gerät (bei Ausschluss ausgehenden Datenverkehrs).

Statistikbefehle

Das Präfix -S gibt an, dass der Befehl zur Befehlsgruppe Statistik gehört.

Befehl kesl-control --app-info

Mit diesem Befehl können Sie Informationen zur Anwendung ausgeben.

Befehlssyntax

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

Argumente und Schlüssel

`--json` – Gibt die Einstellungen im JSON-Format aus.

Befhel kesl-control --supported-tech-info

Zeigt eine Liste mit den Funktionen der Anwendung und Informationen zu deren Status (verwendet oder nicht verwendet) an. Darüber hinaus zeigt der Befehl die Linux-Technologien an, welche zur Bereitstellung der Anwendungsfunktionen verwendet werden.

Befehlssyntax

```
kesl-control [-S] --supported-tech-info [--json]
```

Argumente und Schlüssel

`--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.

Befehlssyntax

```
kesl-control [-S] --get-statistic [--files] [--processes] [--mountpoints]
```

Argumente und Schlüssel

`[--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 Mountpunkte. 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.

Befehlssyntax

```
kesl-control [-S] --omsinfo --file <Dateipfad>
```

Befehle zur Anzeige von Ereignissen

Befehl 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.

Befehlssyntax

```
kesl-control -W [--query "<Filterbedingungen>"]
```

Argumente und Schlüssel

`<Filterbedingungen>` gibt einen oder mehrere logische Ausdrücke im Format `<Feld> <Vergleichsoperation> '<Wert>'` an, die mit dem logischen Operator `and` kombiniert werden, um bestimmte aktuelle Ereignisse auszugeben.

Befehle zur Verwaltung der Ereignisse der Anwendung

Das Präfix -E zeigt an, dass der Befehl zu den Befehlen zur Verwaltung von Programmereignissen gehört (Ereignisse über die Befehlszeile anzeigen, Ereignisse in Kaspersky Security Center anzeigen).

Befehl 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.

Befehlssyntax

```
Befehl 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.

Befehlssyntax

```
kesl-control -E --query "<Filterbedingungen>" [--db <Datenbankdatei>] [-n <Anzahl>] [--file <Dateipfad>] [--json] [--reverse]
```

Argumente und Schlüssel

`<Datenbankdatei>` – Vollständiger Pfad zur Datenbankdatei des Ereignisprotokolls, aus dem Sie Ereignisse ausgeben möchten. Standardmäßig speichert die Anwendung 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.

Mit `<Filterbedingungen>` werden ein oder mehrere logische Ausdrücke im Format `<Feld> <Vergleichsoperation> '<Wert>'` angegeben, die mit dem logischen Operator `and` kombiniert werden, um Abfrageergebnisse einzuschränken.

`<Anzahl>` ist die Anzahl der letzten Ereignisse aus der Auswahl (Einträge, gezählt ab dem Ende der Auswahl), die angezeigt werden sollen.

Wobei `--file <Dateipfad>` dem vollständigen Pfad zu der Datei entspricht, in die Sie die Ereignisse ausgeben möchten. Wenn Sie den Dateinamen eingeben, ohne einen Dateipfad vorzugeben, wird die Datei im aktuellen Verzeichnis erstellt. Ist unter dem gewünschten Pfad bereits eine Datei mit gleichem Namen vorhanden, wird diese überschreiben. Falls das von Ihnen vorgegebene Verzeichnis auf der Festplatte nicht existiert, wird die Datei nicht erstellt.

Wenn Sie den Schalter `--file` nicht angeben, wir die Liste der Ereignisse in die Konsole ausgegeben.

`--json` – Gibt die Ereignisse im JSON-Format aus.

`--reverse` – Ereignisse in umgekehrter Reihenfolge anzeigen (das neueste Ereignis steht oben und das ältesten unten).

Befehle zur Verwaltung der Lizenzschlüssel

Das Präfix -L gibt an, dass der Befehl zur Gruppe der Befehle zur Verwaltung von Lizenzschlüsseln gehört.

> Befehle zum Hinzufügen und Löschen von Lizenzschlüsseln können nur ausgeführt werden, wenn die Anwendung im Standard-Modus oder im Modus als Endpoint Detection and Response Agent verwendet wird. Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird, schlagen die Befehle zur Verwaltung von Lizenzschlüsseln mit einem Fehler fehl. Sie aktivieren die Anwendung als Teil der Lösung Kaspersky Security for Virtualization Light Agent; Sie müssen die Anwendung nicht separat aktivieren.

Befehl kesl-control --add-active-key

Mit diesem Befehl können Sie der Anwendung mithilfe einer Schlüsseldatei oder eines Aktivierungscodes einen aktiven Lizenzschlüssel hinzufügen.

Mit diesem Befehl können Sie sowohl Haupt-Lizenzschlüssel für die Anwendung als auch für Lizenzschlüssel für zusätzliche Funktionen hinzufügen. Der Schlüsseltyp muss nicht im Befehl angeben werden.

Befehlssyntax

```
kesl-control [-L] --add-active-key <Pfad zur Schlüsseldatei>

kesl-control [-L] --add-active-key <Aktivierungscode>
```

Argumente und Schlüssel

`<Pfad zur Schlüsseldatei>` ist der Pfad zur Schlüsseldatei. Wenn sich die Schlüsseldatei im aktuellen Verzeichnis befindet, ist die Angabe des Dateinamens ausreichend.

`<Aktivierungscode>` ist der Aktivierungscode.

Beispiel:
So fügen Sie einen Schlüssel mithilfe der Datei /home/test/00000001.key als aktiven Schlüssel hinzu:

```
kesl-control --add-active-key /home/test/00000001.key
```

Befehl kesl-control --add-reserve-key

Mit diesem Befehl können Sie mithilfe einer Schlüsseldatei oder eines Aktivierungscodes einen Reserve-Lizenzschlüssel zur Anwendung hinzufügen.

Mit diesem Befehl können Sie sowohl Haupt-Lizenzschlüssel für die Anwendung als auch für Lizenzschlüssel für zusätzliche Funktionen hinzufügen. Der Schlüsseltyp muss nicht im Befehl angeben werden.

Wenn der Anwendung auf dem Gerät noch kein aktiver Schlüssel hinzugefügt wurde, schlägt der Befehl fehl.

Befehlssyntax

```
kesl-control [-L] --add-reserve-key <Pfad zur Schlüsseldatei>

kesl-control [-L] --add-reserve-key <Aktivierungscode>
```

Argumente und Schlüssel

`<Pfad zur Schlüsseldatei>` ist der Pfad zur Schlüsseldatei. Wenn sich die Schlüsseldatei im aktuellen Verzeichnis befindet, ist die Angabe des Dateinamens ausreichend.

`<Aktivierungscode>` ist der Aktivierungscode.

Beispiel:
So fügen Sie einen Reserveschlüssel mithilfe der Datei /home/test/00000002.key hinzu:

```
kesl-control --add-reserve-key /home/test/00000002.key
```

Befehl kesl-control --remove-active-key

Mit diesem Befehl können Sie einen aktiven Lizenzschlüssel löschen.

Befehlssyntax

```
kesl-control [-L] --remove-active-key [--edr-optimum]

kesl-control [-L] --remove-active-key [--kuma]

kesl-control [-L] --remove-active-key [--mdr]

kesl-control [-L] --remove-active-key [--edr-kata]
```

Argumente und Schlüssel

`--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).

Wenn Sie in der Befehlszeile die Option `--edr-optimum`, `--kuma`, `--mdr` oder `--edr-kata` nicht angeben, entfernt der Befehl den primären aktiven Schlüssel aus der App.

Befehl kesl-control --remove-reserve-key

Mit diesem Befehl können Sie einen Reserve-Lizenzschlüssel löschen.

Befehlssyntax

```
kesl-control [-L] --remove-reserve-key [--edr-optimum]

kesl-control [-L] --remove-reserve-key [--kuma]

kesl-control [-L] --remove-reserve-key [--mdr]

kesl-control [-L] --remove-reserve-key [--edr-kata]
```

Argumente und Schlüssel

`--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).

Wenn Sie in der Befehlszeile die Option `--edr-optimum`, `--kuma`, `--mdr` oder `--edr-kata` nicht angeben, entfernt der Befehl den primären Reserveschlüssel aus der App.

Befehl kesl-control -L --query

Mit dem Befehl `-L --query` können Sie Informationen über die Lizenz, mit der die Anwendung aktiviert wurde, und die verwendeten Lizenzschlüssel ausgeben.

Befehlssyntax

```
kesl-control -L --query [--json]
```

Argumente und Schlüssel

`--json` – Gibt Daten im JSON-Format aus.

Befehl kesl-control --load-mdr-blob

Der Befehl `--load-mdr-blob` lädt eine BLOB-Datei auf das Gerät hoch, die zur Integration mit Kaspersky Managed Detection and Response verwendet werden kann. Die BLOB-Datei befindet sich im ZIP-Archiv der MDR-Konfigurationsdatei.

Befehlssyntax

```
kesl-control [-L] --load-mdr-blob <Dateipfad MDR-BLOB>
```

Befehl kesl-control --remove-mdr-blob

Der Befehl `--remove-mdr-blob` löscht vom Gerät die BLOB-Datei, die zur Integration mit Kaspersky Managed Detection and Response verwendet werden kann.

Befehlssyntax

```
kesl-control [-L] --remove-mdr-blob
```

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.

Befehlssyntax

```
kesl-control [-F] --add-rule [--name <Regelname>] [--action <Aktion>] [--protocol
<Protokoll>] [--direction <Richtung>] [--remote <Remote-Adresse>[:<Portbereich>]] [--
local <lokale Adresse>[:<Portbereich>]] [--at <Index>]
```

Argumente und Schlüssel

`--name <Regelname>` ist der Name der Netzwerkpaketregel.

`--action <Aktion>` – Aktion, die mit den in dieser Netzwerkpaketregel angegebenen Verbindungen ausgeführt wird.

`--protocol <Protokoll>` ist der Typ des Kommunikationsprotokolls, für das Sie die Netzwerkaktivität überwachen möchten.

`--direction <Richtung>` – Richtung der überwachten Netzwerkaktivität.

`--remote <Remote-Adresse>[:<Portbereich>]` ist die Netzwerkadresse des Remote-Geräts.

`--local <lokale Adresse>[:<Portbereich>]` ist die Netzwerkadresse des Geräts mit Kaspersky Endpoint Security.

`--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.

Befehlssyntax

```
kesl-control [-F] --del-rule --name <Regelname>
```

```
kesl-control [-F] --del-rule --index <Index>
```

Argumente und Schlüssel

`--name <Regelname>` 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.

Befehlssyntax

```
kesl-control [-F] --move-rule --name <Regelname> --at <Index>

kesl-control [-F] --move-rule --index <Index> --at <Index>
```

Argumente und Schlüssel

`--name <Regelname>` 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.

Befehlssyntax

```
kesl-control [-F] --add-zone --zone <Zone> --address <Adresse>
```

Argumente und Schlüssel

`--zone <Zone>` – Vordefinierter Name der Netzwerkzone.

`--address <Adresse>` – Netzwerkadresse oder Subnetz.

Befehl kesl-control --del-zone

Mit diesem Befehl können Sie eine Adresse aus der Netzwerkzone löschen.

Befehlssyntax

```
kesl-control [-F] --del-zone --zone <Zone> --address <Adresse>

kesl-control [-F] --del-zone --zone <Zone> --index <Adressindex>
```

Argumente und Schlüssel

`--zone <Zone>` – Vordefinierter Name der Netzwerkzone.

`--address <Adresse>` – Netzwerkadresse oder Subnetz.

`--index <Adressindex>` ist die Nummer der Adresse in der Netzwerkzone.

Befehl kesl-control -F --query

Mit diesem Befehl können Sie die Firewall-Regeln anzeigen, die mithilfe von Kaspersky Endpoint Security erstellt wurden.

Befehlssyntax

```
Befehl kesl-control -F --query
```

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.

Befehl kesl-control --get-blocked-hosts

Mit diesem Befehl können Sie die Liste der blockierten Geräte in die Konsole ausgeben.

Befehlssyntax

```
kesl-control [-H] --get-blocked-hosts
```

Befehl kesl-control --allow-hosts

Mit diesem Befehl können Sie gesperrte Geräte entsperren.

Befehlssyntax

```
kesl-control [-H] --allow-hosts <Adresse>
```

Argumente und Schlüssel

`<Adresse>` 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 Verwaltung der Gerätekontrolle

Das Präfix D gibt an, dass der Befehl zur Gruppe der Befehle zur Verwaltung der Gerätekontrolle gehört.

Befehl kesl-control --get-device-list

Dieser Befehl gibt eine Liste der Geräte aus, die auf dem Client-Gerät installiert sind oder mit ihm verbunden sind. Die Liste der angeschlossenen Geräte wird im JSON-Format exportiert.

Befehlssyntax

```
kesl-control [-D] --get-device-list [--all] [--json] [--export <Datei>]
```

Argumente und Schlüssel

`--all` – Gibt eine Liste aller verbundenen Geräte aus.

`--json` – Gibt eine Liste aller verbundenen Geräte im JSON-Format aus.

`--export <Datei>` exportiert die Liste der verbundenen Geräte in eine Datei im Format einer Liste vertrauenswürdiger Geräte. Sie müssen den vollständigen Pfad zur Datei im JSON-Format angeben.

Befehl kesl-control --trusted-devices

Mit diesem Befehl können Sie die Liste der vertrauenswürdigen Geräte anzeigen, Geräte hinzufügen und entfernen sowie eine Liste vertrauenswürdiger Geräte aus einer Datei importieren.

Befehlssyntax

```
kesl-control [-D] --trusted-devices [--list] [--add <ID>] [--delete <ID>] [--merge|--
add|--replace --file <Datei>]
```

Argumente und Schlüssel

`--list` – Gibt eine Liste der vertrauenswürdigen Geräte aus.

`--add <ID>` fügt ein Gerät anhand der Geräte-ID oder der Geräte-ID-Maske zur Liste der vertrauenswürdigen Geräte hinzu.

`--delete <ID>` entfernt ein Gerät anhand der Geräte-ID oder der 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 <Datei>` importiert eine Liste vertrauenswürdiger Geräte aus der angegebenen Datei. Sie müssen den vollständigen Pfad zur Datei im JSON-Format angeben.

Befehl kesl-control --request-temporary-device-access

Mit diesem Befehl können Sie eine Zugriffsanfrage-Datei erstellen, um temporären Zugriff auf ein gesperrtes Gerät anzufordern.

Befehlssyntax

```
kesl-control [-D] --request-temporary-device-access --device-id <Geräte-ID> --access-duration <Dauer des Zugriffs> --path <Pfad zur Zugriffsanfrage-Datei>
```

Argumente und Schlüssel

`--device-id <Geräte-ID>` – ID des gesperrten Geräts, auf das Sie zugreifen möchten.

`--access-duration <Dauer des Zugriffs>` – Dauer des Intervalls, für welches Sie Zugriff auf das Gerät bekommen möchten (in Stunden). Mögliche Werte: 1 – 100.

`--path <Pfad zur Zugriffsanfrage-Datei>` – Pfad zum Verzeichnis, in dem Sie die Zugriffsanfrage-Datei mit key-Erweiterung speichern möchten.

Befehl kesl-control --upload-temporary-device-access-key

Mit diesem Befehl können Sie einen Zugriffsschlüssel hochladen, um temporären Zugriff auf ein gesperrtes Gerät zu erhalten.

Befehlssyntax

```
kesl-control [-D] --upload-temporary-device-access-key --path <Pfad zur Datei mit dem Zugriffsschlüssel>
```

Argumente und Schlüssel

`--path <Pfad zur Datei mit Zugriffsschlüssel>` – Pfad zur Datei mit dem Zugriffsschlüssel für das Gerät (Datei mit acode-Erweiterung).

Befehle zur Verwaltung der Programmkontrolle

Das Präfix -A gibt an, dass der Befehl zur Gruppe der Befehle zur Verwaltung der Programmkontrolle gehört.

Befehl kesl-control --get-app-list

Mit diesem Befehl können Sie die Liste der Anwendungen ausgeben, die während der Ausführung der Aufgabe "Inventarisierung" auf dem Client-Gerät erkannt wurden.

Befehlssyntax

```
kesl-control [-A] --get-app-list [--json]
```

Argumente und Schlüssel

`--json` – Gibt Daten im JSON-Format aus.

Befehl kesl-control --get-categories

Mit diesem Befehl können Sie die Liste der erstellten Kategorien der Programmkontrolle ausgeben.

Befehlssyntax

```
kesl-control [-A] --get-categories [--names <Name der Kategorie 1> <Name der Kategorie 2> ... <Name der Kategorie N>] [--file <Pfad zur Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`<Name der Kategorie 1> <Name der Kategorie 2> ... <Name der Kategorie N>` sind die Namen der Kategorien, zu denen Sie Informationen anzeigen möchten. Wenn Sie Informationen mehrerer Kategorien anzeigen möchten, geben Sie die Kategorienamen durch ein Leerzeichen getrennt an.

`--file <Pfad zur Konfigurationsdatei>` ist der vollständige Pfad zur JSON-Konfigurationsdatei, in die die Einstellungen geschrieben werden.

`--json` – Gibt Daten im JSON-Format aus.

Befehl kesl-control --set-categories

Mit diesem Befehl können Sie die Liste der erstellten Kategorien der Programmkontrolle erstellen oder ändern.

Befehlssyntax

```
kesl-control [-A] --set-categories [--names <Name der Kategorie 1> <Name der Kategorie 2> ... <Name der Kategorie N>] --file <Pfad zur Konfigurationsdatei>
```

Argumente und Schlüssel

`<Name der Kategorie 1> <Name der Kategorie 2> ... <Kategoriename N>` sind die Namen der Kategorien, deren Informationen Sie ändern möchten. Wenn Sie Informationen mehrerer Kategorien ändern möchten, geben Sie die Kategorienamen durch ein Leerzeichen getrennt an. Wenn Sie keinen Kategorienamen angeben, wird diese aus der Liste entfernt.

`--file <Pfad zur Konfigurationsdatei>` ist der Pfad zur Konfigurationsdatei mit den Kategorieeinstellungen.

Befehl kesl-control --get-settings 21

Mit diesem Befehl können Sie die Liste der erstellten Regeln der Programmkontrolle ausgeben.

Befehlssyntax

```
kesl-control --get-settings 21 [--file <Pfad zur Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`--file <Pfad zur Konfigurationsdatei>` ist der vollständige Pfad zur Konfigurationsdatei, in die die Einstellungen geschrieben werden.

`--json` – Gibt Daten im JSON-Format aus.

Befehl kesl-control --set-settings 21

Mit dem Befehl können Sie die Liste der erstellten Programmkategorien und Regeln der Programmkontrolle ändern.

Befehlssyntax

```
kesl-control --set-settings 21 [--file <Pfad zur Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`--file <Pfad zur Konfigurationsdatei>` ist der vollständige Pfad zur Konfigurationsdatei, aus der die Einstellungen importiert werden.

`--json` – Importiert die Daten aus einer Datei im JSON-Format importiert.

Befehl kesl-control --set-to-default 21

Mit dem Befehl können Sie die Liste der Programmkategorien und Regeln der Programmkontrolle löschen.

Befehlssyntax

```
kesl-control --set-settings 21 --set-to-default
```

Befehle zur Verwaltung der Web-Kontrolle

Befehl kesl-control --get-settings 26

Mit dem Befehl können Sie eine Liste der konfigurierten Parameter der Web-Kontrolle anzeigen.

Befehlssyntax

```
kesl-control --get-settings 26 [--file <Pfad zur Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`--file <Pfad zur Konfigurationsdatei>` ist der vollständige Pfad zur Konfigurationsdatei, in die die Einstellungen geschrieben werden.

`--json` – Gibt Daten im JSON-Format aus.

Befehl kesl-control --set-settings 26

Mit dem Befehl können Sie eine Liste der konfigurierten Parameter der Web-Kontrolle ändern.

Befehlssyntax

```
kesl-control --set-settings 26 [--file <Pfad zur Konfigurationsdatei>] [--json]
```

Argumente und Schlüssel

`--file <Pfad zur Konfigurationsdatei>` ist der vollständige Pfad zur Konfigurationsdatei, aus der die Einstellungen importiert werden.

`--json` – Importiert die Daten aus einer Datei im JSON-Format importiert.

Befehl kesl-control --set-to-default 26

Mit dem Befehl können Sie die konfigurierten Parameter der Web-Kontrolle löschen und die Werte der Einstellungen auf die Standardregel zurücksetzen.

Befehlssyntax

```
kesl-control --set-settings 26 --set-to-default
```

Befehle zur Backup-Verwaltung

Das Präfix -B zeigt an, dass der Befehl zur Gruppe von Befehlen gehört, die zur Verwaltung des Backup-Speichers verwendet werden.

kesl-control -B --mass-remove

Mit diesem Befehl können Sie alle oder nur bestimmte Objekte aus dem Backup löschen.

Befehlssyntax

Alle Objekte löschen:

```
kesl-control -B --mass-remove
```

Objekte löschen, die den Filterbedingungen entsprechen:

```
kesl-control -B --mass-remove --query "<Filterbedingungen>"
```

Argumente und Schlüssel

Mit `<Filterbedingungen>` werden ein oder mehrere logische Ausdrücke im Format `<Feld> <Vergleichsoperation> '<Wert>'` angegeben, die mit dem logischen Operator `and` kombiniert werden, um Abfrageergebnisse einzuschränken.

Befehl kesl-control -B --query

Mit diesem Befehl können Sie Informationen zu Backup-Objekten ausgeben.

Befehlssyntax

Informationen zu allen Backup-Objekten ausgeben:

```
kesl-control -B --query [-n <Anzahl>] [--json] [--reverse]
```

Informationen zu Backup-Objekten ausgeben, die den Filterbedingungen entsprechen:

```
kesl-control -B --query ["<Filterbedingungen>"] [-n <Anzahl>] [--json] [--reverse]
```

Argumente und Schlüssel

Mit `<Filterbedingungen>` werden ein oder mehrere logische Ausdrücke im Format `<Feld> <Vergleichsoperation> '<Wert>'` angegeben, die mit dem logischen Operator `and` kombiniert werden, um Abfrageergebnisse einzuschränken. Wenn Sie keine Filterbedingungen angeben, zeigt die Anwendung Informationen zu allen Backup-Objekten an.

`<Anzahl>` ist die Anzahl der neuesten Objekte, die angezeigt werden sollen. Wenn Sie den Schalter `-n` nicht angeben, werden die letzten 30 Objekte ausgegeben. Um alle Objekte anzuzeigen, geben Sie den Wert 0 ein.

`--json` – Gibt Daten im JSON-Format aus.

`--reverse` – Objekte in umgekehrter Reihenfolge anzeigen (das neueste Objekt steht oben und das ältesten unten).

Befehl kesl-control -B --restore

Mit diesem Befehl können Sie ein Objekt aus dem Backup wiederherstellen.

Befehlssyntax

```
kesl-control -B --restore <Objekt-ID> [--file <Dateipfad>]
```

Argumente und Schlüssel

`<Objekt-ID>` ist die ID des Objekts im Backup.

`--file <Dateipfad>` ist der neue Name der Datei und der Pfad zu dem Verzeichnis, in dem die Datei gespeichert werden soll. Wenn Sie den Schalter `--file` nicht angeben, wird das Objekt mit seinem ursprünglichen Namen an seinem ursprünglichen Speicherort wiederhergestellt.

Befehle zur Verwaltung der Quarantäne

Das Präfix -Q zeigt an, dass der Befehl zur Gruppe von Befehlen gehört, die zur Verwaltung der Quarantäne verwendet werden.

Befehl kesl-control -Q --mass-remove

Mit diesem Befehl können Sie alle oder nur bestimmte Dateien aus der Quarantäne löschen.

Befehlssyntax

Alle Dateien löschen:

```
Befehl kesl-control -Q --mass-remove
```

Dateien löschen, die den Filterbedingungen entsprechen:

```
kesl-control -Q --mass-remove --query "<Filterbedingungen>"
```

Argumente und Schlüssel

Mit `<Filterbedingungen>` werden ein oder mehrere logische Ausdrücke im Format `<Feld> <Vergleichsoperation> '<Wert>'` angegeben, die mit dem logischen Operator `and` kombiniert werden, um Abfrageergebnisse 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.

Befehlssyntax

```
kesl-control [-Q] --put <Dateipfad> [--md5] [--sha256] [--save-original-file]
```

Argumente und Schlüssel

< Dateipfad > – Pfad 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.

Befehlssyntax

Informationen zu allen Quarantäne-Dateien anzeigen:

```
kesl-control -Q --query [-n <Anzahl>] [--json]
```

Informationen zu den Quarantäne-Dateien anzeigen, die den Filterbedingungen entsprechen:

```
kesl-control -Q --query ["<Filterbedingugnen>"] [-n <Anzahl>]
```

Argumente und Schlüssel

Mit < Filterbedingungen > werden ein oder mehrere logische Ausdrücke im Format < Feld > < Vergleichsoperation > '< Wert >' angegeben, die mit dem logischen Operator and kombiniert werden, um Abfrageergebnisse einzuschränken. Wenn Sie keine Filterbedingungen angeben, zeigt die Anwendung Informationen zu allen Quarantäne-Dateien an.

< Zahl > 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.

Befehlssyntax

```
kesl-control -Q --restore <Objekt-ID> [--file <Dateipfad>]
```

Argumente und Schlüssel

< Datei-ID > – ID der Datei in der Quarantäne.

`--file <Dateipfad>` 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 Anwendung 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 von Benutzern und Rollen

-U – Präfix, das angibt, dass der Befehl zur Gruppe von Befehlen zur Verwaltung von Benutzern und Rollen gehört

Befehl kesl-control --get-user-list

Mit diesem Befehl können Sie die Liste der Benutzer und Rollen ausgeben.

Befehlssyntax

```
kesl-control [-U] --get-user-list
```

Befehl kesl-control --grant-role

Mit diesem Befehl können Sie einem bestimmten Benutzer eine Rolle zuweisen.

Befehlssyntax

```
kesl-control [-U] --grant-role <Rolle> <Benutzer>
```

Befehl kesl-control --revoke-role

Mit diesem Befehl können Sie einem bestimmten Benutzer eine Rolle entziehen.

Befehlssyntax

```
kesl-control [-U] --revoke-role <Rolle> <Benutzer>
```

Befehle zur Verwaltung von EDR Expert (on-premise)

-R – ein Präfix, das angibt, dass der Befehl zur Befehlsgruppe für die Verwaltung der Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA) und Kaspersky Endpoint Detection and Response Expert (on-premise) und Kaspersky Endpoint Detection and Response Optimum 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.

Befehlssyntax

```
kesl-control [-R] --add-kataedr-server-certificate <Datei> [--server-type
<response|telemetry>]
```

Argumente und Schlüssel

`<Datei>` – Pfad zur Datei, die das Serverzertifikat enthält.

`--server-type <response|telemetry>` – Beim Integrationsmodus "EDR Expert (OSMP)": der jeweilige Server, dessen Zertifikat hinzugefügt oder geändert werden soll:

- `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.

Befehlssyntax

```
kesl-control [-R] --remove-kataedr-server-certificate [--server-type
<response|telemetry>]
```

Argumente und Schlüssel

`--server-type <response|telemetry>` – Beim Integrationsmodus "EDR Expert (OSMP)": der jeweilige Server, dessen Zertifikat gelöscht werden soll:

- `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.

Befehlssyntax

```
kesl-control [-R] --query-kataedr-server-certificate [--server-type <response|telemetry>]
```

Argumente und Schlüssel

`--server-type <response|telemetry>` – Beim Integrationsmodus "EDR Expert (OSMP)": der jeweilige Server, für dessen Zertifikat Informationen ausgegeben werden sollen:

- `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.

Befehlssyntax

```
kesl-control [-R] --add-kataedr-client-certificate <Datei> [--server-type
<response|telemetry>]
```

Argumente und Schlüssel

`<Datei>` ist der Pfad zum Crypto-Container (PFX-Archiv), der das Client-Zertifikat und den privaten Schlüssel enthält.

`--server-type <response|telemetry>` – Beim Integrationsmodus "EDR Expert (OSMP)": der jeweilige Server, für den das Client-Zertifikat hinzugefügt werden soll:

- `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.

Befehlssyntax

```
kesl-control [-R] --remove-kataedr-client-certificate [--server-type
<response|telemetry>]
```

Argumente und Schlüssel

`--server-type <response|telemetry>` – Beim Integrationsmodus "EDR Expert (OSMP)": der jeweilige Server, für den das Client-Zertifikat gelöscht werden soll:

- `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.

Befehlssyntax

```
kesl-control [-R] --query-kataedr-client-certificate [--server-type <response|telemetry>]
```

Argumente und Schlüssel

`--server-type <response|telemetry>` – Beim Integrationsmodus "EDR Expert (OSMP)": der jeweilige Server, für den das Client-Zertifikat gelöscht werden soll:

- `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 von NDR (KATA)

-R – ein Präfix, das angibt, dass der Befehl zur Befehlsgruppe für die Verwaltung der Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA) und Kaspersky Endpoint Detection and Response Expert (on-premise) und Kaspersky Endpoint Detection and Response Optimum gehört.

Befehl kesl-control --add-katandr-server-certificate

Mit diesem Befehl können Sie ein zuvor hinzugefügtes Zertifikat des NDR-Servers hinzufügen oder ersetzen.

Befehlssyntax

```
kesl-control [-R] --add-katandr-server-certificate <Datei>
```

Argumente und Schlüssel

`<Datei>` – Pfad zur Datei, die das Serverzertifikat enthält.

Befehl kesl-control --remove-katandr-server-certificate

Mit diesem Befehl wird ein NDR-Serverzertifikat entfernt.

Befehlssyntax

```
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.

Befehlssyntax

```
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.

Befehlssyntax

```
kesl-control [-R] --add-katandr-client-certificate <Datei>
```

Argumente und Schlüssel

`<Datei>` ist der Pfad zum Crypto-Container (PFX-Archiv), der das Client-Zertifikat und den privaten Schlüssel enthält.

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.

Befehlssyntax

```
kesl-control [-R] --remove-katandr-client-certificate
```

Befehl kesl-control --query-katandr-client-certificate

Mit diesem Befehl können Sie Informationen zum Client-Zertifikat ausgeben.

Befehlssyntax

```
kesl-control [-R] --query-katandr-client-certificate
```

Befehle zur Verwaltung der Netzwerkisolation eines Geräts

-R – ein Präfix, das angibt, dass der Befehl zur Befehlsgruppe für die Verwaltung der Integrationseinstellungen mit Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA) und Kaspersky Endpoint Detection and Response Expert (on-premise) und Kaspersky Endpoint Detection and Response Optimum 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.

Befehlssyntax

```
kesl-control [-R] --isolation-stat
```

Befehl kesl-control --isolation-off

Mit diesem Befehl können Sie die Netzwerkisolation des Geräts temporär deaktivieren.

Befehlssyntax

```
kesl-control [-R] --isolation-off
```

Befehle 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.

Befehlssyntax

```
kesl-control [-M] --add-kuma-server-certificate <Dateipfad>
```

Argumente und Schlüssel

`<Dateipfad>` – Pfad zu der Datei, die das Serverzertifikat enthält.

Befehl kesl-control --remove-kuma-server-certificate

Mit diesem Befehl können Sie das Zertifikat des KUMA-Servers löschen.

Befehlssyntax

```
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.

Befehlssyntax

```
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.

Befehlssyntax

```
kesl-control [-M] --add-kuma-client-certificate <Dateipfad>
```

Argumente und Schlüssel

`<Dateipfad>` – Name und Pfad des Crypto-Containers (Archiv im pfx-Format), der den geheimen Schlüssel enthält.

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.

Befehlssyntax

```
kesl-control [-M] --remove-kuma-client-certificate
```

Befehl kesl-control --query-kuma-client-certificate

Mit diesem Befehl können Sie Informationen zum Client-Zertifikat ausgeben.

Befehlssyntax

```
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.

Befehlssyntax

```
kesl-control [-X] --add-sandbox-server-certificate <Datei>
```

Argumente und Schlüssel

< Datei > – Pfad zur Datei, die das Serverzertifikat enthält.

Befehl kesl-control --remove-sandbox-server-certificate

Mit dem Befehl können Sie ein Zertifikat des Servers, der die Interaktion mit Sandbox gewährleistet, löschen.

Befehlssyntax

```
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.

Befehlssyntax

```
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.

Befehlssyntax

```
kesl-control [-X] --add-sandbox-client-certificate < Datei >
```

Argumente und Schlüssel

< Datei > ist der Pfad zum Crypto-Container (PFX-Archiv), der das Client-Zertifikat und den privaten Schlüssel enthält.

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.

Befehlssyntax

```
kesl-control [-X] --remove-sandbox-client-certificate
```

Befehl kesl-control --query-sandbox-client-certificate

Mit diesem Befehl können Sie Informationen zum Client-Zertifikat ausgeben.

Befehlssyntax

```
kesl-control [-X] --query-sandbox-client-certificate
```

Befehl kesl-control --sandbox

Mit diesem Befehl können Sie Dateien zur Untersuchung an Sandbox senden.

Befehlssyntax

```
kesl-control [-X] --sandbox <Pfad 1> <Pfad 2>
```

Argumente und Schlüssel

`<Pfad>` – Pfad zu der Datei oder dem Verzeichnis, das Sie überprüfen 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.

Befehlssyntax

```
kesl-control [-T] --scan-ioc --path  <Pfad zu Verzeichnis oder Datei>  [--process on|off]
[--hint <regulärer Ausdruck>] [--arpentry on|off] [--ports on|off] [--system on|off] [--
files on|off] [--drives all|system|critical|custom] [--excludes <Liste der Ausschlüsse>]
[--scope <Liste der Verzeichnisse>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

Argumente und Schlüssel

`--path <Pfad zum Verzeichnis oder zur Datei>` 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 <regulärer Ausdruck>` 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 <Liste der Ausnahmen>` ist die Liste der Pfade, die von Untersuchungen ausgeschlossen sind.

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 <Liste der Verzeichnisse>` 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 der **kritischen Bereiche** durch.
  - /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.

Befehle der Anwendung im Light Agent-Modus zum Schutz virtueller Umgebungen

Das Präfix -V gibt an, dass der Befehl zur Gruppe der Befehle von Kaspersky Endpoint Security gehört, die im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet werden (als Bestandteil von Kaspersky Security for Virtualization Light Agent).

Diese Befehle können nur ausgeführt werden, wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird.

Befehl kesl-control --ksvla-info

Mit diesem Befehl können Sie Informationen zur Nutzung der Anwendung im Light Agent-Modus zum Schutz virtueller Umgebungen ausgeben.

Befehlssyntax

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

Befehl kesl-control --viis-info

Mit diesem Befehl können Sie Informationen über die Verbindung des Light Agents (d. h. von Kaspersky Endpoint Security, das als Light Agent im Rahmen von Kaspersky Security for Virtualization Light Agent verwendet wird) zum Integrationsserver ausgeben.

Befehlssyntax

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

Befehl kesl-control --svm-info

Mit diesem Befehl können Sie Informationen über die Verbindung des Light Agents (d. h. von Kaspersky Endpoint Security, das als Light Agent im Rahmen von Kaspersky Security for Virtualization Light Agent verwendet wird) zur SVM ausgeben.

Befehlssyntax

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

Befehle zur Verwaltung der Sammlung von Kennzahlen zum Systemzustand

Befehl kesl-control --export-metrics

Mit dem Befehl können Sie die Sammlung von Kennzahlen zum Status des Betriebssystems konfigurieren.

Befehlssyntax

```
kesl-control [-J] --export-metrics [--period <Intervall zwischen den Exporten in Sekunden>|--interactive]
```

Argumente und Schlüssel

`--period` – periodisches Intervall für die Ausgabe der Ergebnisse an die Befehlszeile

`<Zeitintervall zwischen den Ausgaben in Sekunden>` – periodisches Intervall für die Ausgabe der Ergebnisse an die Befehlszeile (in Sekunden)

`--interactive` – interaktive Ausgabe (durch Drücken der **`Eingabetaste`**)

Anhang 2. Konfigurationsdateien und Standardeinstellungen der App

Zur Verwaltung der Ausführung von Kaspersky Endpoint Security werden die folgenden Konfigurationsdateien verwendet:

- Konfigurationsdateien, welche die Einstellungen für die Erstkonfiguration der Anwendung enthalten:
  - Konfigurationsdatei autoinstall.ini, die bei der Installation der Anwendung mithilfe von Kaspersky Security Center verwendet wird.
  - Konfigurationsdatei, die bei der Installation der Anwendung über die Befehlszeile verwendet wird.
- 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.

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 in diesen Dateien die Werte der Einstellungen ändern.

Es wird empfohlen, die Änderung der Standardwerte unter Anleitung von Spezialisten des Technischen Supports nach den von ihnen erhaltenen Anweisungen vorzunehmen.

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 Anwendungspakets. 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. Der Parameter wird während der Erstkonfiguration der Anwendung konfiguriert.	`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. Der Parameter wird während der Erstkonfiguration der Anwendung konfiguriert.	`true/yes` – Anwendung wird im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet `false/no` – das Programm wird im Standard-Modus verwendet.
`EndpointAgentMode`	Verwendung von Kaspersky Endpoint Security im Modus als Endpoint Detection and Response Agent.	`true/yes` – Die Anwendung wird im Modus als Endpoint Detection and Response Agent verwendet. `false/no` – das Programm wird im Standard-Modus verwendet.
`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.	`true/yes` – Die Anwendung wird innerhalb der Lösung "Kaspersky Container Security" als Komponente zum Schutz vor bedrohlichen Dateien verwendet. `false/no` (Standardwert) bedeutet, dass die Anwendung in einem der Modi von Kaspersky Endpoint Security verwendet wird (Standard-Modus, Modus als Endpoint Detection and Response Agent oder Light Agent-Modus zum Schutz virtueller Umgebungen).
`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.

Einstellung	Description	Werte
`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.
`CoreDumps`	Aktiviert die Erstellung einer Dump-Datei im Falle eines Absturzes der Anwendung.	`true/yes`, um eine Dump-Datei zu erstellen, wenn die App abstürzt. `false/no` (Standardwert), um keine Dump-Datei zu erstellen, wenn die 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.
`MinFreeDiskSpace`	Die minimale Größe an Festplattenspeicher, die nach dem Schreiben der Dump-Datei verbleiben soll, in Megabyte.	Standardwert: 300.
`ScanMemoryLimit`	Maximaler Speicherverbrauch durch die Anwendung 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.
`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: 2047.
`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.

Einstellung	Description	Werte
`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.	Standardwert: 3.
`SafeMode`	Aktivieren des "abgesicherten" Ausführungsmodus der Anwendung 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.	`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.
`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.	`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.
Der Abschnitt **[Network]** enthält die folgenden Einstellungen:		

Einstellung	Description	Werte
`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).
`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 von der Anwendung erstellt oder bereits untersucht wurden, damit diese nicht im Protokoll des Tools "iptable" aufgenommen werden.	Der Wert wird als Dezimal- oder Hexadezimalzahl mit vorangestelltem 0x angegeben. Der Standardwert ist 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 vor Dateien und Prozessen nicht aktivieren.

Einstellung	Description	Werte
`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:		
`ServerMode`	Rolle einer geschützten virtuellen Maschine, auf der Kaspersky Endpoint Security im Light Agent-Modus zum Schutz virtueller Umgebungen verwendet wird: Server oder Workstation. Es wird nicht empfohlen, den Wert dieses Parameters manuell zu ändern. Der Parameter wird während der Erstkonfiguration der Anwendung konfiguriert.	`true/yes` – Die virtuelle Maschine wird als Server verwendet. `false/no` – Die virtuelle Maschine wird als Workstation verwendet.
`VdiMode`	Aktivieren des Modus zum Schutz von VDI-Infrastrukturen bei Verwendung der Anwendung im Light Agent-Modus zum Schutz virtueller Umgebungen. Es wird nicht empfohlen, den Wert dieses Parameters manuell zu ändern. Der Parameter wird während der Erstkonfiguration der Anwendung konfiguriert.	`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.

Einstellung	Description	Werte
`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.
`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. `< Wert >%` – ein Wert zwischen 1 und 100 Prozent des Arbeitsspeichers. `< Wert >MB` – ein Wert in Megabyte. `lowest/< Wert >%/< Wert >MB` – der kleinere Wert aus Prozentwert und absolutem Wert in Megabyte. `highest/< Wert >%/< Wert >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. `< Wert >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. `< Wert >%` – ein Wert zwischen 0 und 100 Prozent des Arbeitsspeichers. `< Wert >MB` – ein Wert in Megabyte. `lowest/< Wert >%/< Wert >MB` – der kleinere Wert aus Prozentwert und absolutem Wert in Megabyte. `highest/< Wert >%/< Wert >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

Einstellung	Description	Werte
`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
`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.
Der Abschnitt **[Environment]** ist in der Konfigurationsdatei standardmäßig nicht vorhanden.		

Einstellung	Description	Werte
`ExperimentalContainerdSupport`	Aktivierung der Unterstützung für die containerd-Umgebung, wenn die Komponente zur Container-Überwachung ausgeführt wird (ContainerScan, Container-Überwachung). Diese Einstellung ist standardmäßig nicht in der Konfigurationsdatei vorhanden. Wenn Sie beim Ausführen der Komponente "Container-Überwachung" die Umgebung "containerd" verwenden möchten, müssen Sie in der Konfigurationsdatei den Abschnitt `[Environment]` manuell hinzufügen und ihn um den Parameter `ExperimentalContainerdSupport` ergänzen.	`true/yes` – Unterstützung 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=Nein

ScanSfxArchived=Nein

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

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

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

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=Erlauben

DefaultIncomingPacketAction=Erlauben

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
```

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
```

Allgemeine Anwendungseinstellungen

Die allgemeinen Anwendungseinstellungen bestimmen die Ausführung der Anwendung als Ganzes und die Ausführung einzelner Funktionen.

Allgemeine Anwendungseinstellungen

Parameter	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 Anwendung erforderlich.	Standardmäßig ist das Standardverzeichnis der Samba-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 Anwendung erforderlich.	Standardmäßig ist das Standardverzeichnis der NFS-Konfigurationsdatei angegeben. Standardwert: /etc/exports
`TraceLevel`	Aktiviert die Anwendungsprotokollierung und den Detaillierungsgrad der Protokolldateien.	`Detailed` – detaillierteste Protokolldateien erstellen. `MediumDetailed` – Protokolldatei mit Info- und Fehlermeldungen erstellen `NotDetailed` – Protokolldatei mit Fehlermeldungen erstellen `None` (Standardwert) – Keine Protokolldatei erstellen.

Parameter	Description	Werte
`TraceFolder`	Verzeichnis, in dem die Protokolldateien der Anwendung gespeichert sind. Nach der Änderung dieser Einstellung ist ein Neustart der Anwendung erforderlich.	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--------`).
`TraceMaxFileCount`	Gibt die Maximalanzahl der Protokolldateien der Anwendung an. Nach der Änderung dieser Einstellung ist ein Neustart der Anwendung erforderlich.	1 bis 10000 Standardwert: 10.
`TraceMaxFileSize`	Legt die maximale Größe der Protokolldatei der Anwendung fest (in Megabyte). Nach der Änderung dieser Einstellung ist ein Neustart der Anwendung erforderlich.	1 bis 1000 Standardwert: 500.
`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.	4096–33554432 Standardwert: 16384.
`DetectOtherObjects`	Aktiviert die Erkennung legaler Programme, die von Angreifern zur Beschädigung von Geräten oder Daten ausgenutzt werden können.	`Yes` – Aktiviert die Erkennung legaler Programme, die von Angreifern zur Beschädigung von Geräten oder Daten ausgenutzt werden können. `No` (Standardwert) – Deaktiviert die Erkennung legaler Programme, die von Angreifern zur Beschädigung von Geräten oder Daten ausgenutzt werden können.

Parameter	Description	Werte
`NamespaceMonitoring`	Aktivieren der Untersuchung von Namespaces und Containern (Untersuchung von Containern, Container-Überwachung). 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) – Untersuchung von Namensräumen und Containern aktivieren. `No` – Untersuchung von Namensräumen und Containern deaktivieren.
`FileBlockDuringScan`	Aktivieren des Modus des Interceptors von Dateioperationen mit Blockieren des Zugriffs auf Dateien während der Untersuchung. Der Modus des Interceptors von Dateioperationen hat Auswirkungen auf die Ausführung der Komponenten Schutz vor bedrohlichen Dateien und Gerätekontrolle.	`Yes` (Standardwert) – Zugriff auf Dateien während des Untersuchung blockieren. `No` – Zugriff auf Dateien während des Untersuchung nicht blockieren. Der Zugriff auf eine beliebige Datei ist erlaubt, die Überprüfung erfolgt im asynchronen Modus. Dieser Modus des Interceptors von Dateioperationen hat während der Ausführung weniger Auswirkungen auf die Systemleistung. Es besteht jedoch das Risiko, dass eine Bedrohung in einer Datei nicht desinfiziert oder entfernt wird, wenn diese Datei beispielsweise während der Untersuchung ihren Namen ändert, bevor die Anwendung eine Entscheidung über den Status dieser Datei treffen kann. In diesem Fall werden unabhängig davon, welcher Ausführungsmodus festgelegt ist, die Komponenten Schutz vor bedrohlichen Dateien, Gerätekontrolle und Ausführungsprävention von Objekten im Benachrichtigungs-Modus ausgeführt.
`UseKSN`	Verwendung von Kaspersky Security Network während der Anwendungsausführung konfigurieren	`Standard` — Verwendung von Kaspersky Security Network im Standard-Modus aktivieren. `Erweitert` — Verwendung von Kaspersky Security Network im erweiterten Modus aktivieren. `Nein` (Standardwert) — Kaspersky Security Network nicht 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` – Aktivieren des Ausführungsmodus, in dem Kaspersky Endpoint Security eine schlankere Version der Malware-Datenbanken verwendet. `No` (Standardwert) – vollständige Malware-Datenbanken verwenden. Der Cloud-Modus wird automatisch deaktiviert, wenn KSN deaktiviert ist.

Parameter	Description	Werte
`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.	`Yes` – die Komponente "Managed Detection and Response" aktivieren. `No` (Standardwert) – die Komponente "Managed Detection and Response" deaktivieren
`UseEdrOptimum`	Aktivieren der Komponente "EDR Optimum" für die Integration mit Kaspersky Endpoint Detection and Response Optimum.	`Ja` — Komponente „EDR Optimum“ aktivieren. `Nein` (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.	`Ja`: Nutzung eines Proxy-Servers aktivieren. `Nein` (Standardwert) — Nutzung eines Proxy-Servers deaktivieren.

Parameter	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 Formate: • `[<Verbindungsprotokoll>://]<IP-Adresse des Proxyservers>:<Port>`, wenn für die Verbindung mit dem Proxyserver keine Authentifizierung erforderlich ist; • `[<Verbindungsprotokoll>://][<Benutzername>:[<Kennwort>]@]<IP-Adresse des Proxyservers>:<Port>`, wenn beim Verbinden mit dem Proxyserver eine Authentifizierung erforderlich ist. Das Herstellen einer Verbindung mit dem Proxyserver über das HTTPS-Protokoll wird nicht unterstützt.
`ProxyBypass`	Liste mit Adressen, für deren Verbindung kein Proxyserver verwendet wird.	Die Adresse wird im Format `<Adresse>[:<Portnummer>` angegeben. Zur Angabe von Adressen können Sie Platzhalter (`*`-Symbole) un Kommentare (nach einem "\"-Symbol) verwenden.
`ProxyBypassEdr`	Verwendung des Proxyservers bei einer Verbindung mit Servern, welche die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) gewährleisten.	`Yes` – Kein Proxyserver für die Verbindung mit Servern verwenden, welche die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) gewährleisten. `No` (Standardwert) – Proxyserver für die Verbindung mit Servern verwenden, welche die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premise) gewährleisten.
`ProxyBypassNdr`	Verwendung des Proxyservers bei einer Verbindung mit Servern, welche die Integration mit Kaspersky Network Detection and Response (KATA) gewährleisten.	`Yes` – Kein Proxyserver für die Verbindung mit Servern verwenden, welche die Integration mit Kaspersky Network Detection and Response (KATA) gewährleisten. `No` (Standardwert) – Proxyserver für die Verbindung mit Servern verwenden, welche die Integration mit Kaspersky Netzwork Detection and Response (KATA) gewährleisten.
`ProxyBypassSandbox`	Verwendung des Proxyservers bei einer Verbindung mit Servern, welche die Integration mit Sandbox gewährleisten.	`Yes` – Kein Proxyserver für die Verbindung mit Servern verwenden, welche die Integration mit Sandbox gewährleisten. `No` (Standardwert) – Proxyserver für die Verbindung mit Servern verwenden, welche die Integration mit Sandbox gewährleisten.
`MaxEventsNumber`	Maximale Anzahl von Ereignissen, die von der Anwendung gespeichert werden. Wenn die angegebene Anzahl von Ereignissen übertroffen wird, löscht die Anwendung die ältesten Ereignisse.	Standardwert: 500000. Wenn der Wert auf "0" gesetzt ist, werden keine neuen 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 starten kann, nicht beschränkt.	0 bis 100000 0 – Ein nicht berechtigter Benutzer kann Aufgaben zur benutzerdefinierten Untersuchung nicht starten. Standardwert: 5.
`UseSyslog`	Aktivieren der Aufzeichnung von Anwendungsereignissen in syslog. Für den Zugriff auf syslog sind Root-Rechte erforderlich.	`Yes` – Protokollieren von Ereignissen im syslog aktivieren. `No` (Standardwert) – Protokollieren von Ereignissen im syslog deaktivieren.

Parameter	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/events.d
`ExcludedMountPoint.item_#`	Der Mountpunkt, den Sie vom Untersuchungsbereich ausschließen möchten. Die Ausnahme gilt für den Betrieb der Komponenten Schutz vor bedrohlichen Dateien, Schutz vor Verschlüsselung, Container-Überwachung (Untersuchung von Containern, Container-Überwachung) sowie für die Aufgabe Untersuchung von Wechseldatenträgern und wird auch für die Ausführung der Untersuchungsaufgaben ODS und 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, die auf dem Gerät über SMB- oder NFS-Protokolle gemountet sind, werden vom Modul zum Abfangen von Dateioperationen ausgeschlossen. `Mounted:NFS` – Alle Remote-Verzeichnisse, die auf dem Gerät über NFS-Protokolle gemountet sind, werden vom Modul zum Abfangen von Dateioperationen ausgeschlossen. `Mounted:SMB` – Alle Remote-Verzeichnisse, die auf dem Gerät über SMB-Protokolle gemountet sind, werden vom Modul zum Abfangen von Dateioperationen ausgeschlossen. `Mounted:< Typ des Dateisystems >` – alle eingebundenen Verzeichnisse mit dem angegebenen Dateisystem werden vom Modul zum Abfangen von Dateioperationen ausgeschlossen. `/mnt` — Objekte im Mountpunkt /mnt (einschließlich Unterverzeichnissen) vom Abfangen von Dateioperationen ausschließen. Dieses Verzeichnis wird als temporärer Mountpunkt für Wechseldatenträger verwendet. `< Pfad, der die Maske /mnt/user* oder /mnt/**/user_share>` enthält — Objekte in Mountpunkten, deren Namen die angegebene **Maske** enthalten, vom Abfangen von Dateioperationen ausschließen. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- ode Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeiche (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Um den Mountpunkt `/dir` auszuschließen, müssen Sie genau `/dir` (ohne die Sternchen) angeben. Die Maske `/dir/*` schließt alle Mountpunkte eine Ebene tiefer als `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Die Maske `/dir/**` schließt alle Mountpunkte auf allen Verschachtelungsebenen unter `/dir` aus, aber nicht den Mountpunkt `/dir` selbst. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.

Parameter	Description	Werte
`MemScanExcludedProgramPath.item_#`	Prozess-Speicher von der Untersuchung ausschließen. Der Arbeitsspeicher des angegebenen Prozesses wird von der Anwendung nicht untersucht.	`< vollständiger Pfad zum Prozess >` – Prozess im angegebenen lokalen Verzeichnis nicht untersuchen. Bei der Angabe des Pfades können Sie **Masken** verwenden. Verwenden Sie das Zeichen `*` (Sternchen), um eine Maske für Datei- oder Verzeichnisnamen zu erstellen. Sie können einen Stern `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) vor dem Zeichen `/` im Datei- oder Verzeichnisnamen zu ersetzen. Beispiel: `/dir/*/file` oder `/dir/*/*/file`. Sie können zwei aufeinander folgende Sterne `*` verwenden, um eine beliebige Anzahl an Zeichen (inklusive einer leeren Menge) im Datei- oder Verzeichnisnamen, einschließlich des Zeichens `/` zu ersetzen. Beispiel: `/dir/**/file*/` oder `/dir/file**/`. Die Maske `**` kann nur ein einziges Mal pro Verzeichnisname verwendet werden. Beispiel: Die Maske `/dir/**/**/file` ist nicht korrekt. Sie können das Symbol `?` anstelle eines einzelnen Zeichens in einem Datei- oder Verzeichnisnamen verwenden.
`UseOnDemandCPULimit`	Aktiviert die Begrenzung der Nutzung von CPU-Ressourcen für die Aufgabentypen *ODS*, *ContainerScan* und *InventoryScan*.	`Yes` – Aktiviert die Begrenzung der Nutzung von CPU-Ressourcen für die Aufgabentypen *ODS*, *ContainerScan* und *InventoryScan*. `No` (Standardwert) – Deaktiviert die Begrenzung der Nutzung von CPU-Ressourcen für Aufgaben.
`OnDemandCPULimit`	Maximale Auslastung aller Prozessorkerne (in Prozent) bei der Ausführung der Aufgabentypen *ODS*, *ContainerScan* und *InventoryScan*.	Eine Ganzzahl zwischen 10 und 100. Standardwert: 100.
`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 – 999999 0 – Die Größe des Backups ist nicht begrenzt. Standardwert: 0.
`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.	Standardwert: /var/opt/kaspersky/kesl/common/objects-backup/ Für den Zugriff auf das Standardverzeichnis sind Root-Rechte erforderlich.

Parameter	Description	Werte
`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 – 999999 0 – Die Größe der Quarantäne ist nicht begrenzt. Standardwert: 200, wenn die Anwendung im Standardmodus verwendet wird, und 100, wenn die Anwendung im Light Agent-Modus verwendet wird.
`ShowPopUpNotifications`	Aktivieren der Anzeigen von Pop-up-Benachrichtigungen in der grafischen Benutzeroberfläche.	`Yes` (Standardwert) – In der grafischen Benutzeroberfläche werden Pop-up-Benachrichtigungen angezeigt. `No` – In der grafischen Benutzeroberfläche werden keine Pop-up-Benachrichtigungen angezeigt.
`PowerSaveMode`	Abbrechen geplanter Aufgaben auf einem, das im Akkubetrieb läuft.	`Ja` (Standardwert) – Geplante Aufgaben auf einem Gerät, das im Akkubetrieb läuft, überspringen. `Nein` – Geplante Aufgaben auf einem Gerät unabhängig von der Stromquelle (Netz oder Akku) planmäßig ausführen.
`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.	`UseFanotify` (Standardwert) – fanotify-Technologie zum Abfangen von Systemereignissen verwenden. `UseUpdatableKernelModule` – Aktualisierbares Kernel-Modul zum Abfangen von Systemereignissen verwenden.
`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 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.

Parameter	Description	Werte
`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 Wert) – 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.
`SystemEventsTransmission`	Aktivieren der Aufzeichnung von Informationen über Ereignisse von Dritthersteller-Anwendungen in syslog. Für den Zugriff auf syslog sind Root-Rechte erforderlich.	`Yes` – Protokollieren von Informationen über Ereignisse von Dritthersteller-Anwendungen in syslog aktivieren. `No` (Standardwert) – Protokollieren von Informationen über Ereignisse von Dritthersteller-Anwendungen in syslog deaktivieren

Allgemeine Einstellungen der Untersuchung von Containern

Die allgemeinen Einstellungen für die Untersuchung von Containern werden verwendet, wenn Namespaces und Container in Echtzeit untersucht werden (Untersuchung von Containern, Container-Überwachung).

Allgemeine Einstellungen für die Untersuchung von Containern und Namensräumen

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.

Parameter	Description	Werte
`UseDocker`	Verwendung des Systems zur Verwaltung von Docker-Containern. Es wird die Integration mit dem System zur Verwaltung von Docker-Containern der Version 28.5.2 und niedriger unterstützt.	`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`	Verwendung der CRI-O-Umgebung.	`Yes` (Standardwert) – CRI-O-Umgebung verwenden `No` – CRI-O-Umgebung nicht verwenden
`CrioConfigFilePath`	Der Pfad zur CRI-O-Konfigurationsdatei.	Standardwert: /etc/crio/crio.conf.
`UsePodman`	Verwendung des Podman-Tools.	`Yes` (Standardwert) – Podman-Tool verwenden `No` – Podman-Tool nicht verwenden
`PodmanBinaryPath`	Pfad zur ausführbaren Datei des Podman-Tools.	Der Standardwert ist /usr/bin/podman.
`PodmanRootFolder`	Pfad zum Stammverzeichnis des Container-Speichers.	Der Standardwert ist /var/lib/containers/storage.
`UseRunc`	Verwendung des runc-Tools.	`Yes` (Standardwert) – runc-Tool verwenden `No` – runc-Tool nicht verwenden
`RuncBinaryPath`	Pfad zur ausführbaren Datei des runc-Tools.	Der Standardwert ist /usr/bin/runc.
`RuncRootFolder`	Pfad zum Stammverzeichnis des Speichers für den Container-Status.	Der Standardwert ist /run/runc.

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 Anwendung entschlüsselt den verschlüsselten Datenverkehr nicht.
`EncryptedConnectionsScanErrorAction`	Legt die Aktion der Anwendung 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 Anwendung 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.

Parameter	Description	Werte
`UntrustedCertificateAction`	Aktion, welche die Anwendung ausführen soll, wenn sie ein nicht vertrauenswürdiges Zertifikat erkennt.	`Allow` (Standardwert) – Netzwerkverbindung zulassen, die beim Aufruf einer Domain mit einem nicht vertrauenswürdigen Zertifikat hergestellt wurde `Block` – Netzwerkverbindung blockieren, die beim Aufruf einer Domain mit einem nicht vertrauenswürdigen Zertifikat hergestellt wurde
`ManageExclusions`	Verwendung von Ausschlüssen bei der Untersuchung von verschlüsseltem Datenverkehr.	`Yes` – Websites, die im Abschnitt `[Exclusions.item_#]` angegeben sind (s. unten), nicht untersuchen `No` (Standardwert) – Alle Websites untersuchen
`MonitorNetworkPorts`	Legt fest, auf welche Weise Kaspersky Endpoint Security Netzwerkports überwacht.	`Selected` (Standardwert) – Nur Netzwerkports überwachen, die im Abschnitt `[NetworkPorts.item_#]` angegeben sind (siehe unten) `All` – Alle Netzwerkports überwachen Die Angabe dieses Wertes kann die Auslastung des Betriebssystems erheblich erhöhen.
`NetInterceptorMode`	Modus zum Abfangen des Datenverkehrs in der Kaspersky Endpoint Security.	`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 Anwendung überwachen soll.	`1 – 65535` Der Standardwert ist nicht angegeben.

Einstellungen des Aufgabenzeitplans

In der folgenden Tabelle werden die Einstellungen des Aufgabenzeitplans beschrieben, die Sie für alle Programmaufgaben verwalten können.

Einstellungen des Aufgabenzeitplans

Parameter	Description	Werte
`RuleType`	Zeitplan für den Aufgabenstart	`Once` – Führt die Aufgabe einmal aus. `Monthly` – Führt die Aufgabe jeden Monat am angegebenen Tag und zur angegebenen Uhrzeit aus. `Weekly` – Führt die Aufgabe jede Woche am angegebenen Tag und zur angegebenen Uhrzeit aus. `Daily` – Führt die Aufgabe regelmäßig in einem angegebenen Intervall in Tagen aus. `Hourly` – Führt die Aufgabe regelmäßig in einem angegebenen Intervall in Stunden aus, beginnend mit dem angegebenen Datum und der angegebenen Uhrzeit. `Minutely` – Führt die Aufgabe regelmäßig in einem angegebenen Intervall in Minuten aus, beginnend mit der angegebenen Uhrzeit. `Manual` – Aufgabe manuell starten. `PS` – Aufgabe nach dem Starten der Anwendung starten. `BR` – Aufgabe nach dem Update der Anwendungsdatenbanken starten.
`StartTime`	Datum und Uhrzeit des Aufgabenstarts. Die Einstellung `StartTime` ist erforderlich, wenn die Einstellung `RuleType` einen der folgenden Werte hat: Once, Monthly, Weekly, Daily, Hourly, Minutely.	`[< Jahr >/< Monat >/< Tag des Monats >] [ hh ]:[ mm ]:[ ss ]; [< Tag des Monats >| < Wochentag >]; [< Starthäufigkeit >]`
`RandomInterval`	Zeitintervall (in Minuten) von 0 bis zum angegebenen Wert, welches zur Startzeit der Aufgabe hinzugefügt wird, um den gleichzeitigen Start von Aufgaben zu vermeiden.	Standardwert: 99 Minuten.
`RunMissedStartRules`	Start einer übersprungenen Aufgabe nach dem Starten der Anwendung.	`Yes` (Standardwert) – Aktiviert den Start einer übersprungenen Aufgabe nach dem Starten der Anwendung. `No` – Aktiviert nicht den Start einer übersprungenen Aufgabe nach dem Starten der Anwendung.
`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.

Anhang 3. Rückgabecodes der Befehlszeile

Kaspersky Endpoint Security enthält die folgenden Rückgabecodes der Befehlszeile.

0 – Befehl/Aufgabe erfolgreich ausgeführt

1 – Allgemeiner Fehler in den Syntax des Befehls

2 – Fehler in den übergebenen Anwendungseinstellungen

64 – Kaspersky Endpoint Security wurde nicht gestartet

66 – Programmdatenbanken sind nicht geladen (wird nur vom Befehl `kesl-control --app-info` verwendet).

67 – Aktivierung 2.0 wurde aufgrund von Netzwerkproblemen fehlerhaft abgeschlossen

68 – Befehlsausführung unmöglich, da die Anwendung durch die Verwaltung einer Richtlinie ausgeführt wird

69 – Die Anwendung befindet sich in der Infrastruktur von Amazon Paid Ami

70 – Versuch, eine bereits laufende Aufgabe zu starten, eine laufende Aufgabe zu löschen, die Einstellungen einer laufenden Aufgabe zu ändern, eine beendete Aufgabe zu beenden, eine angehaltene Aufgabe anzuhalten oder eine laufende Aufgabe fortzusetzen

71 – Erklärung zu Kaspersky Security Network nicht akzeptiert

72 – Fund von Bedrohungen während der Ausführung der Aufgabe "Benutzerdefinierte Untersuchung" oder "Benutzerdefinierte Untersuchung von Containern"

73 – Versuch, die Einstellungen der Aufgabe „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 oder die Aufgabe kann nicht ausgeführt werden, da die Anwendung im Light Agent-Modus verwendet wird

79 – Der Befehl kann nicht ausgeführt werden, da die Anwendung im Standard-Modus verwendet wird

80 – Das Herunterladen des Updates ist aufgrund von Netzwerkproblemen fehlgeschlagen

128 – Unbekannter Fehler

65 – Alle übrigen Fehler

Anhang 4. Einstellungen für die Zusammenarbeit mit Kaspersky Anti-Virus für Linux Mail Server

So passen Sie die gemeinsame Ausführung von Kaspersky Endpoint Security und Kaspersky Anti-Virus für Linux Mail Server an:

1. Speichern Sie die Einstellungen der Aufgabe zum Schutz vor bedrohlichen Dateien in der Konfigurationsdatei mithilfe des folgenden Befehls:

   `kesl-control --get-settings 1 --file <vollständiger Dateipfad>`

2. Öffnen Sie die erstellte Konfigurationsdatei zum Bearbeiten.

3. Fügen Sie der erstellten Datei folgenden Abschnitt hinzu:

   `[ExcludedFromScanScope.item_<Elementnummer>]`

   `Path=/var/opt/kaspersky/klms`

4. Wiederholen Sie den oben genannten Abschnitt für alle Mail-Agenten, die mit Kaspersky Anti-Virus für Linux Mail Server integriert wurden.

5. Um das temporäre Verzeichnis für Filter und Dienste von Kaspersky Anti-Virus für Linux Mail Server von der Untersuchung auszuschließen, fügen Sie der erstellten Datei folgenden Abschnitt hinzu:

   `[ExcludedFromScanScope.item_<Elementnummer>]`

   `Path=/tmp/klmstmp`

6. Speichern Sie die Änderungen in der Konfigurationsdatei.

7. Importieren Sie die Einstellungen aus der Konfigurationsdatei in die Aufgabe zum Schutz vor bedrohlichen Dateien mithilfe des folgenden Befehls:

   `kesl-control --set-settings 1 --file <vollständiger Dateipfad>`

Anhang 5. Anwendungsparameter in der Richtlinie in der Web Console

Dieser Abschnitt enthält Beschreibungen der Richtlinieneinstellungen in der Web Console auf der Registerkarte **„Anwendungseinstellungen“**.

Geräteschutz vor Bedrohungen

Schutz vor bedrohlichen Dateien

Für Windows, macOS und Linux

Die Komponente „Schutz vor bedrohlichen Dateien“ schützt das Dateisystem des Computers vor einer Infektion. Standardmäßig befindet sich die Komponente Schutz vor bedrohlichen Dateien permanent im Arbeitsspeicher des Computers und untersucht in Echtzeit alle Dateien, die geöffnet, gespeichert oder ausgeführt werden. Die Komponente untersucht Dateien auf allen Computerlaufwerken, einschließlich der angeschlossenen Laufwerke. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der heuristischen Analyse.

Die Komponente untersucht die Dateien, auf die der Benutzer oder ein Programm zugreift. Beim Fund einer schädlichen Datei blockiert Kaspersky Endpoint Security den Vorgang mit dieser Datei. Das Programm desinfiziert oder löscht die schädliche Datei. Das Vorgehen ist von den Einstellungen der Komponente „Schutz vor bedrohlichen Dateien“ abhängig.

Beim Zugriff auf eine Datei, deren Inhalte sich im OneDrive-Cloud-Speicher befinden, lädt Kaspersky Endpoint Security den Inhalt dieser Datei herunter und untersucht ihn.

`Linux` Für Linux-Geräte ist die Komponente davon abhängig, in welchem Modus der Dateizugriff während Untersuchungen blockiert wird. Diesen Modus können Sie in den allgemeinen Programmeinstellungen auswählen. Während der Untersuchung wird der Zugriff auf eine Datei standardmäßig blockiert.

Einstellungen für Datei-Anti-Virus

Einstellungen	Betriebssystem	Beschreibung
Untersuchungsausnahmen	`Windows` `macOS` `Linux`	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. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

Einstellungen	Betriebssystem	Beschreibung
Aktion beim Fund einer Bedrohung	`Windows` `macOS` `Linux`	**Desinfizieren – Löschen, wenn Desinfektion fehlschlägt**. 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 (je nach Betriebssystem)**. `Windows` `Linux` Wenn diese Option ausgewählt ist, versucht das Programm automatisch, die erkannte infizierte Datei zu desinfizieren. Wenn die Desinfektion fehlschlägt, wird die Datei durch die Anwendung blockiert. **Blockieren oder Aktion erfragen (je nach Betriebssystem)**. `Windows` `Linux` Wenn diese Option ausgewählt ist, blockiert das Programm automatisch die infizierte Datei, ohne zu versuchen, sie zu desinfizieren oder zu löschen. `macOS` Kaspersky Endpoint Security zeigt ein Benachrichtigungsfenster mit Informationen über den Typ des schädlichen Objekts an, mit dem die Datei infiziert wurde, und fordert den Benutzer auf, die von Kaspersky Endpoint Security auszuführende Aktion auszuwählen. Die verfügbaren Aktionen können je nach Objektstatus variieren. Vor dem Desinfizieren oder Löschen einer infizierten Datei erstellt das Programm eine Backup-Kopie der Datei für den Fall, dass sie später wiederhergestellt werden muss oder eine Desinfektion möglich wird.
Schutzbereich	`Windows` `macOS` `Linux`	Enthält die Objekte, die von der Komponente „Schutz vor bedrohlichen Dateien“ untersucht werden. Ein Untersuchungsobjekt kann sein: Festplatte, Wechseldatenträger oder Netzwerklaufwerk, Ordner, eine Datei oder mehrere Dateien, die durch eine Maske angegeben sind. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht standardmäßig die Dateien, die von beliebigen Festplatten, Wechseldatenträgern und Netzlaufwerken aus gestartet werden. Der Schutzbereich dieser Objekte kann nicht geändert oder gelöscht werden. Sie können nur ein Objekt (z. B. Wechseldatenträger) von der Untersuchung ausschließen. `Linux` Für Linux-Geräte können Sie Untersuchungsbereiche mithilfe der Komponente „Schutz vor bedrohlichen Dateien“ ändern oder entfernen. Geben Sie mindestens einen Überwachungsbereich an, damit die Komponente funktioniert.
File types	`macOS`	**Scan all files**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security ausnahmslos alle Dateien (unabhängig von Format und Erweiterung). **Scan applications and documents by content**. Bei Auswahl dieser Option untersucht das Programm nur potenziell infizierbare Dateien. Bevor eine Datei auf Schadcode untersucht wird, wird die interne Kopfzeile im Hinblick auf das Dateiformat analysiert (z. B. txt, doc, exe). Während der Untersuchung werden auch Dateien mit bestimmtem Dateierweiterungen gesucht. **Scan applications and documents by extension**. Bei Auswahl dieser Option untersucht das Programm nur potenziell infizierbare Dateien. Das Dateiformat wird auf Basis der Dateierweiterung ermittelt.
Untersuchung optimieren	`Windows` `macOS`	Unter **Untersuchung optimieren** können Sie Kaspersky Endpoint Security so konfigurieren, dass bei der Untersuchung von Dateien eine höhere Leistung erreicht wird. • `Windows` `macOS` **Nur neue und veränderte Dateien untersuchen**. Untersucht nur neue Dateien und jene Dateien, die seit ihrer letzten Untersuchung verändert wurden. Dadurch lässt sich die Untersuchungsdauer reduzieren. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien. • `Windows` **Container anhalten, falls Desinfektion fehlschlägt**. Das Programm hat möglicherweise keine ausreichenden Lese- und Schreibrechte für das gefundene Objekt. In diesem Fall kann das erkannte Objekt nicht desinfiziert oder gelöscht werden. Wenn dieses Kontrollkästchen aktiviert ist, blockiert das Programm das erkannte Objekt und hält den Container an. Wenn dieses Kontrollkästchen deaktiviert ist, blockiert das Programm nur das erkannte Objekt. • `macOS` **Untersuchung von Systemlaufwerken ohne Schreibzugriff überspringen**. Wenn das Kontrollkästchen aktiviert ist, untersucht das Programm das schreibgeschützte Systemvolume nicht. Dadurch wird die Untersuchungszeit erheblich verkürzt. • `Windows` **Dateivorgänge, die in Windows-Containern ausgeführt werden, nicht untersuchen**. Wenn dieses Kontrollkästchen aktiviert ist, untersucht das Programm den Container nur, wenn der Container gestartet wird. Wenn das Kontrollkästchen deaktiviert ist, untersucht das Programm den Container kontinuierlich in Echtzeit.

Einstellungen	Betriebssystem	Beschreibung
Untersuchung von zusammengesetzten Dateien	`Windows` `macOS` `Linux`	Eine häufig anzutreffende Methode zum Verstecken von Viren und anderen gefährlichen Programmen ist die Einbettung der Schädlinge in zusammengesetzte Dateien wie beispielsweise Archive oder Datenbanken. Um Viren und andere Bedrohungen zu erkennen, die auf diese Weise verborgen sind, muss die zusammengesetzte Datei entpackt werden, wodurch die Untersuchung verlangsamt werden kann. Sie können die Typen der zusammengesetzten Dateien, die untersucht werden sollen, beschränken und dadurch die Untersuchungsgeschwindigkeit erhöhen. • **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. • **Programmpakete und selbstextrahierende Archive**. Untersuchung von Installationspaketen für Drittanbieter-Anwendungen und von selbstextrahierenden Archiven. Selbstentpackende Archive sind Archive, die ein ausführbares Modul zum Entpacken enthalten. Damit selbstextrahierende Archive untersucht werden, müssen Sie das Kontrollkästchen **Archive untersuchen** aktivieren. • `Windows` `macOS` **Dateien im Office-Format und eingebettete OLE-Objekte**. Untersuchung von Microsoft Office-Dateien (z. B. doc, docx, xls, ppt) und in Dateien eingebetteten OLE-Objekten (z. B. Excel-Tabellen, Makros, E-Mail-Anhänge). • `Windows` `Linux` **E-Mail-Datenbanken untersuchen**. Untersuchung von E-Mail-Datenbanken für Microsoft Outlook, Outlook Express, The Bat! und andere E-Mail-Programme. • `Linux` **Dateien in E-Mail-Formaten untersuchen**. Untersuchung von E-Mail-Nachrichtendateien im Nur-Text-Format.
Archive im Hintergrund extrahieren, wenn größer als (MB)	`Windows` `macOS`	Wenn das Kontrollkästchen aktiviert ist, gewährt das Programm den Zugriff auf zusammengesetzte Dateien, deren Größe über dem festgelegten Wert liegt, bevor diese Dateien untersucht werden. Dabei entpackt und untersucht Kaspersky Endpoint Security die zusammengesetzten Dateien im Hintergrundmodus. Das Programm gewährt den Zugriff auf zusammengesetzte Dateien, die kleiner sind als der festgelegte Wert. Der Zugriff wird erst gewährt, nachdem diese Dateien entpackt und untersucht wurden. Wenn das Kontrollkästchen deaktiviert ist, gewährt das Programm den Zugriff auf zusammengesetzte Dateien mit beliebiger Größe erst, nachdem die Dateien entpackt und untersucht wurden.
Archive nicht untersuchen, wenn größer als (MB)	`Windows` `macOS` `Linux`	Ist dieses Kontrollkästchen aktiviert, werden zusammengesetzte Dateien, welche die festgelegte Größe überschreiten, nicht untersucht. Ist dieses Kontrollkästchen deaktiviert, werden zusammengesetzte Dateien unabhängig von ihrer Größe durch das Programm untersucht. Große Dateien, die aus Archiven extrahiert werden, werden unabhängig vom Status dieses Kontrollkästchens durch das Programm untersucht.
Datei überspringen, wenn Untersuchung länger dauert als (Sek.)	`Linux`	Wenn das Kontrollkästchen aktiviert ist, beendet das Programm die Untersuchung von zusammengesetzten Dateien nach Ablauf der festgelegten Zeit. Ist der Wert `0` angegeben, dann ist die Untersuchungsdauer nicht beschränkt.
Untersuchung im Hintergrund	`Windows`	Die *Untersuchung im Hintergrund* ist ein Modus von Kaspersky Endpoint Security, in welchem dem Benutzer keine Benachrichtigungen angezeigt werden. Die Untersuchung im Hintergrund erfordert weniger Computerressourcen als andere Untersuchungstypen (z. B. vollständige Untersuchung). In diesem Modus untersucht Kaspersky Endpoint Security die Autostart-Objekte, den Bootsektor, den Systemspeicher und die Systempartition.
Untersuchung aus dem Kontextmenü	`Windows`	Kaspersky Endpoint Security bietet die Möglichkeit, aus dem Kontextmenü bestimmte Dateien auf Viren und andere bedrohliche Programme zu untersuchen. Wenn eine Untersuchung aus dem Kontextmenü ausgeführt wird, werden Dateien, deren Inhalt sich im Cloud-Speicher OneDrive befindet, nicht von Kaspersky Endpoint Security untersucht.

Schutz vor BadUSB-Angriffen

Für Windows und Linux

Bestimmte Viren verändern die in USB-Geräten eingebettete Software so, dass das USB-Gerät vom Betriebssystem als Tastatur erkannt wird. Infolgedessen kann der Virus unter Ihrem Benutzerkonto Befehle ausführen, um z. B. Malware herunterzuladen.

Die Komponente „Schutz vor BadUSB-Angriffen“ verhindert, dass modifizierte USB-Geräte, die eine Tastatur simulieren, mit dem PC verbunden werden.

Wenn ein USB-Gerät an den Computer angeschlossen und vom Betriebssystem als Tastatur erkannt wird, fordert das Programm den Benutzer auf, mit diesem Gerät oder mithilfe der Bildschirmtastatur (falls diese verfügbar ist) einen vom Programm generierten Code einzugeben (siehe nachstehende Abbildung). Dieser Vorgang heißt Autorisierung der Tastatur.

Wenn der Zahlencode korrekt eingegeben wurde, speichert das Programm die Identifikationsparameter der Tastatur (VIP/PID) und die Nummer des Ports, an dem sie angeschlossen wurde in der Liste der autorisierten Tastaturen. Wenn die Tastatur erneut angeschlossen oder das Betriebssystem neu gestartet wird, muss die Tastatur nicht mehr autorisiert werden.

Wenn eine autorisierte Tastatur über einen anderen USB-Port an den Computer angeschlossen wird, fordert das Programm erneut zur Autorisierung dieser Tastatur auf.

Wenn der Code falsch eingegeben wird, generiert die Anwendung einen neuen. Sie können die Anzahl der Versuche für die Eingabe des Zahlencodes konfigurieren. Wird der Zahlencode mehrmals falsch eingegeben oder das Tastatur-Autorisierungsfenster geschlossen (siehe Abbildung unten), blockiert die Anwendung die Eingabe über diese Tastatur. Nach Ablauf der Blockierungszeit für USB-Geräte oder wenn das Betriebssystem neu gestartet wird, schlägt das Programm erneut vor, die Autorisierung vorzunehmen.

Das Programm erlaubt die Verwendung einer autorisierten Tastatur. Eine Tastatur, die nicht autorisiert wurde, wird blockiert.

Die Komponente „Schutz vor BadUSB-Angriffen“ wird standardmäßig nicht installiert. Wenn Sie die Komponente „Schutz vor BadUSB-Angriffen“ benötigen, können Sie die Komponente entweder vor der Programminstallation in den Eigenschaften des Installationspakets hinzufügen oder die Auswahl der Programmkomponenten nach der Programminstallation ändern.

Autorisierung der Tastatur

Einstellungen für den Schutz vor BadUSB-Angriffen

Einstellungen	Betriebssystem	Beschreibung
Maximale Anzahl der Autorisierungsversuche für USB-Geräte	`Windows` `Linux`	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.)	`Windows` `Linux`	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 für die Autorisierung von USB-Geräten verbieten	`Windows` `Linux`	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 für die Autorisierung von USB-Geräten verbieten	`Windows` `Linux`	Wenn der Schalter aktiviert ist, zeigt Kaspersky Endpoint Security keinen Strichcode in der Benachrichtigung zur Strichcode-Scanner-Authentifizierung an.

Untersuchung von Wechseldatenträgern

Für Windows, macOS und Linux

Kaspersky Endpoint Security untersucht alle Dateien, die Sie ausführen oder kopieren, selbst wenn die sich die Datei auf einem Wechseldatenträger befindet (Komponente "Schutz vor bedrohlichen Dateien"). Um die Ausbreitung von Viren und anderer Schadsoftware zu verhindern, können Sie festlegen, dass Wechseldatenträger automatisch untersucht werden, wenn sie mit dem Computer verbunden werden. Kaspersky Endpoint Security versucht automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Schlägt die Desinfektion fehl, werden sie von Kaspersky Endpoint Security gelöscht. Die Komponente sorgt für die Sicherheit eines Computers und nutzt dafür Untersuchungen, die maschinelles Lernen, heuristische Analyse (hohe Ebene) und Signaturanalyse implementieren. Zur Optimierung der Untersuchung verwendet Kaspersky Security zusätzlich die Technologien iSwift und iChecker. Diese Technologien sind immer aktiviert und können nicht deaktiviert werden.

Einstellungen für die Untersuchung von Wechseldatenträgern

Einstellungen	Betriebssystem	Beschreibung
Untersuchungstyp	`Windows` `Linux`	**Schnelle Untersuchung**. Ist diese Option ausgewählt, so untersucht Kaspersky Endpoint Security nach dem Anschließen eines Wechseldatenträgers nur Dateien mit bestimmten Formaten, die als besonders anfällig für Infektionen gelten. Außerdem werden zusammengesetzte Objekte nicht entpackt. **Genaue Untersuchung**. Wenn diese Option ausgewählt ist, untersucht Kaspersky Endpoint Security alle Dateien, wenn ein Wechseldatenträger angeschlossen wird, einschließlich Dateien, die in zusammengesetzten Objekten, Archiven, Programmpaketen und Office-Format-Dateien verschachtelt sind. Kaspersky Endpoint Security untersucht Dateien in Mail-Formaten und kennwortgeschützte Archive nicht.
Benutzern das Anhalten der Untersuchung verbieten	`Windows`	Wenn dieses Kontrollkästchen aktiviert ist, sind für die Aufgabe zur Untersuchung von Wechseldatenträgern in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security die Schaltfläche **Abbrechen** des Abschnitts **Aufgaben** und die Schaltfläche **Abbrechen** des Fensters für die Wechseldatenträger-Untersuchung nicht verfügbar.
Zugriff auf den Wechseldatenträger während der Untersuchung blockieren	`Linux`	Wenn das Kontrollkästchen aktiviert ist, blockiert Kaspersky Endpoint Security den Zugriff auf Dateien auf dem verbundenen Laufwerk, während diese untersucht werden.

Einstellungen	Betriebssystem	Beschreibung
Untersuchungsfortschritt ausblenden	`Windows`	Wenn dieses Kontrollkästchen aktiviert ist, blendet Kaspersky Endpoint Security den Fortschrittsbalken der Untersuchung von Wechseldatenträgern aus. Das Programm führt die Untersuchung im Hintergrund aus. Wenn dieses Kontrollkästchen deaktiviert ist, zeigt Kaspersky Endpoint Security den Fortschritt der Untersuchung von Wechseldatenträgern in einem separaten Fenster und im Abschnitt **Aufgaben** an.
Wechseldatenträger nicht untersuchen, wenn größer als	`Windows`	Ist dieses Kontrollkästchen aktiviert, führt Kaspersky Endpoint Security mit Wechseldatenträgern, deren Größe den Höchstwert nicht überschreitet, die ausgewählte Aktion durch. Wenn die Größe des Wechseldatenträgers den festgelegten Wert überschreitet, überspringt Kaspersky Endpoint Security die Untersuchung. Ist das Kontrollkästchen deaktiviert, führt Kaspersky Endpoint Security mit Wechseldatenträgern die ausgewählte Aktion aus, wobei die Datenträgergröße nicht berücksichtigt wird.

Verhaltensanalyse

Für Windows, macOS und Linux

Die Komponente „Verhaltensanalyse“ empfängt Daten über die Aktionen der Programme auf Ihrem Computer und versorgt andere Schutzkomponenten mit diesen Informationen, um deren Effektivität zu erhöhen. Die Komponente „Verhaltensanalyse“ verwendet Vorlagen für gefährliches Programmverhalten. Stimmt die Aktivität eines Programms mit einer der Aktivitäten aus den Vorlagen für gefährliches Verhalten überein, so führt Kaspersky Endpoint Security die ausgewählte Reaktion aus. Diese Funktionalität von Kaspersky Endpoint Security basiert auf Vorlagen für gefährliches Verhalten und bietet einen proaktiven Computerschutz.

Die Komponente „Verhaltensanalyse“ überwacht zusätzlich Netzwerkports auf das Vorhandensein von Programmprozessen, die den Computer gefährden können. Informationen über solche Vorgänge ruf das Programm aus den Antiviren-Datenbanken ab.

Für eine optimale Leistung der Komponente „Verhaltensanalyse“ wird empfohlen, die Komponente Schutz vor Web-Bedrohungen zu aktivieren.

Einstellungen der Verhaltensanalyse

Einstellungen	Betriebssystem	Beschreibung

Vertrauenswürdige Programme	`Windows`
	`macOS`
	`Linux`
		Die *Liste der vertrauenswürdigen Programme* ist eine Liste mit Programmen, deren Datei- oder Netzwerkaktivität nicht von Kaspersky Endpoint Security überwacht wird (selbst wenn diese schädlich ist). Gleiches gilt für den Zugriff dieser Programme auf die Systemregistrierung. Kaspersky Endpoint Security überwacht standardmäßig alle Objekte, die von einem beliebigen Programmprozess geöffnet, gestartet oder gespeichert werden, und kontrolliert die Aktivität aller Programme sowie den von diesen generierten Netzwerkverkehr. Nachdem eine Programm zur Liste der vertrauenswürdigen Programme hinzugefügt wurde, beendet Kaspersky Endpoint Security die Überwachung der Programmaktivitäten.
		Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

Untersuchungsausnahmen	`Windows`
	`macOS`
	`Linux`
		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.
		Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

Einstellungen	Betriebssystem	Beschreibung
Aktion beim Fund einer Bedrohung	`Windows` `macOS` `Linux`	**Datei löschen oder blockieren (je nach Betriebssystem)**. `Windows` `macOS` Wenn diese Option ausgewählt ist und eine schädliche Aktivität erkannt wird, löscht Kaspersky Endpoint Security die ausführbare Datei des schädlichen Programms und erstellt im Backup eine Kopie der Datei. `Linux` Wenn schädliche Aktivität erkannt wird, blockiert Kaspersky Endpoint Security das Programm, das die schädliche Aktivität ausführt, und protokolliert Informationen über die erkannte schädliche Aktivität. **Informieren**. `Windows` `Linux` Wenn diese Option ausgewählt ist und eine schädliche Programmaktivität erkannt wird, beendet Kaspersky Endpoint Security dieses Programm nicht, sondern fügt Informationen über die schädliche Aktivität dieses Programms zur Liste der aktiven Bedrohungen hinzu. `macOS` Wenn schädliche Aktivität erkannt wird, fragt Kaspersky Endpoint Security den Benutzer, welche Aktion beim Fund einer schädlichen Aktivität ausgeführt werden soll. Die verfügbaren Aktionen können je nach Objektstatus variieren. **Blockieren**. Ist diese Variante ausgewählt, so beendet Kaspersky Endpoint Security beim Fund einer schädlichen Programmaktivität die betreffende Anwendung.

Schutz vor Verschlüsselung

Für Windows, macOS und Linux

`Windows` Auf Windows-Geräten überwacht die Komponente nur Vorgänge für Dateien, die sich auf Ebene des NTFS-Dateisystems befinden und nicht vom EFS-System verschlüsselt wurden.

`Linux` Auf Linux-Geräten analysiert die Komponente die Dateien in lokalen Verzeichnissen mit Netzwerkzugriff über SMB/NFS.

`macOS` Auf macOS-Geräten überwacht die Komponente die SMB-Freigaben.

Die Komponente „Schutz vor Verschlüsselung“ schützt vor Remote-Verschlüsselung. Dazu wird die Aktivität bei Netzwerkfreigaben analysiert. Falls die Aktivität mit einer Vorlage für gefährliches Verhalten übereinstimmt, das für eine externe Verschlüsselung charakteristisch ist, so führt Kaspersky Endpoint Security die ausgewählte Aktion aus.

`Linux` Lesen Sie die Informationen über den Schutz vor Verschlüsselung, bevor Sie die Komponente auf Linux-Geräten aktivieren.

Einstellungen	Betriebssystem	Beschreibung
Untersuchungsausnahmen	`Windows` `Linux`	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. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.
Ausnahmen nach Name oder IP-Adresse	`Windows`	**Namen/IP-Adressen von vertrauenswürdigen Computern**. Liste der Computer, deren Verschlüsselungsversuche für gemeinsame Ordner nicht überwacht werden. **Ausnahmen nach Maske**. Ausnahmen für den Schutzbereich. Indem ein Ordner aus dem Schutzbereich ausgeschlossen wird, lässt sich die Anzahl der Fehlalarme reduzieren, wenn Ihr Unternehmen bei der Dateiübertragung über freigegebene Ordner eine Datenverschlüsselung verwendet. Verwenden Sie **Masken**. • Zeichen `*`, das als Platzhalter für eine beliebige Zeichenkombination steht, die auch leer sein kann. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\*\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung txt, die sich in Ordnern auf Laufwerk C befinden, allerdings nicht in untergeordneten Ordnern. • Zwei aufeinanderfolgende Zeichen `*` ersetzen in einem Datei- oder Ordnernamen eine beliebige Zeichenkombination. Dabei kann der Name auch leer sein und die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden) enthalten. Beispiel: Die Maske `C:\Folder\**\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung TXT, die sich in Ordnern innerhalb des Ordners `Folder` befinden, unter Ausnahme des Ordners `Folder` selbst. Die Maske muss mindestens eine Verschachtelungsebene umfassen. Die Maske `C:\**\*.txt` ist nicht gültig. • Zeichen `?`, das als Platzhalter für ein beliebiges Einzelzeichen steht. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\Folder\???.txt` umfasst die Pfade aller Dateien, die im Ordner mit dem Namen `Folder` enthalten sind, die Erweiterung TXT haben und deren Name aus drei Zeichen besteht.
Aktion beim Fund einer Bedrohung	`Windows` `macOS` `Linux`	**Informieren**. Wenn diese Variante ausgewählt ist und ein Versuch zur Änderung von Dateien in freigegebenen Ordnern erkannt wird, fügt Kaspersky Endpoint Security Informationen über diesen Versuch zur Liste der aktiven Bedrohungen hinzu und fügt dem Bericht einen Eintrag hinzu. **Verbindung blockieren für (Min.)**. `Windows` Wenn diese Option ausgewählt ist und Kaspersky Endpoint Security einen Versuch erkennt, Dateien in freigegebenen Ordnern zu ändern, blockiert das Programm den Zugriff auf die Dateiänderung für die Sitzung, welche die schädliche Aktivität initiiert hat, und erstellt Backup-Kopien der veränderten Dateien. `macOS` `Linux` Wenn Kaspersky Endpoint Security einen Versuch erkennt, Dateien in freigegebenen Ordnern zu ändern, wird der Netzwerkverkehr des Geräts blockiert, das an der schädlichen Aktivität beteiligt ist. Die App generiert das Ereignis *Verschlüsselung erkannt*, das Informationen über das gefährdete Gerät enthält.
Schutzbereich	`Windows` `macOS` `Linux`	Der *Schutzbereich* ist eine Liste mit Pfaden zu freigegebenen Ordnern, für die Kaspersky Endpoint Security die Dateiaktivität überwacht. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske. Standardmäßig werden freigegebene Ordner automatisch identifiziert und die Dateiaktivität wird in allen Ordnern überwacht. `macOS` Kaspersky Endpoint Security schützt alle freigegebenen Ordner für macOS-Geräte. Es ist nicht möglich, den Schutzbereich zu ändern. `Windows` `Linux` Sie können den Schutzbereich auswählen: **Alle freigegebenen Netzwerkordner auf dem geschützten Gerät**. Das Programm überwacht die Dateiaktivität in allen freigegebenen Ordnern. **Nur die angegebenen freigegebenen Ordner**. Das Programm überwacht Verschlüsselungsversuche nur in den angegebenen freigegebenen Ordnern.

Exploit-Prävention

Für Windows, macOS und Linux

Die Komponente „Exploit-Prävention“ überwacht Programmcode, der mithilfe eines Exploits Schwachstellen eines Computers ausnutzt, um dadurch Administratorrechte zu erhalten oder schädliche Aktionen auszuführen. Exploits können beispielsweise einen Angriff mit Überlauf der Zwischenablage verwenden. Dazu sendet der Exploit große Datenvolumen an ein verwundbares Programm. Bei der Verarbeitung dieser Daten führt das verwundbare Programm schädlichen Code aus. Aufgrund dieses Angriffs kann der Exploit eine nicht autorisierte Installation von Schadsoftware starten. Wenn der Startversuch einer ausführbaren Datei aus einem verwundbaren Programm nicht vom Benutzer ausgeführt wurde, blockiert Kaspersky Endpoint Security den Start dieser Datei oder informiert den Benutzer.

Die Komponente „Exploit-Prävention“ überwacht zusätzlich Netzwerkports auf das Vorhandensein von Anwendungsprozessen, die den Computer gefährden können. Informationen über solche Vorgänge ruf das Programm aus den Antiviren-Datenbanken ab.

Damit die Exploit-Prävention ordnungsgemäß funktioniert, muss die Verhaltensanalyse aktiviert sein. Für eine optimale Leistung der Komponente „Exploit-Prävention“ wird empfohlen, auch die Komponente Schutz vor Web-Bedrohungen zu aktivieren.

`Linux` Für Linux-Geräte muss auch das aktualisierbare Kernel-Modul zum Abfangen von Systemereignissen aktiviert werden.

Einstellungen der Exploit-Prävention

Einstellungen	Betriebssystem	Beschreibung
Aktion beim Fund einer Bedrohung	`Windows` `macOS` `Linux`	**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. **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.
Schutz des Arbeitsspeichers von Systemprozessen	`Windows`	Ist dieser Schalter aktiviert, so blockiert Kaspersky Endpoint Security Drittanbieter-Prozesse, die versuchen, auf den Arbeitsspeicher von Systemprozessen zuzugreifen.

Schutz von Verbindungen und Kommunikation über das Netzwerk

Schutz vor E-Mail-Bedrohungen

Für Windows, macOS und Linux

Die Komponente "Schutz vor E-Mail-Bedrohungen" untersucht ein- und ausgehende E-Mail-Anhänge auf Viren und andere Bedrohungen. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der heuristischen Analyse.

Der Schutz vor E-Mail-Bedrohungen kann sowohl eingehende als auch ausgehende Nachrichten untersuchen. Das Programm unterstützt die Protokolle POP3, SMTP, IMAP, NNTP.

`Linux` Das Programm für Linux-Geräte unterstützt das NNTP-Protokoll nicht.

Unterstützte E-Mail-Clients

- `Windows`, `macOS` Microsoft Office Outlook
- `Windows`, `macOS` Mozilla Thunderbird
- `Windows` Windows Mail
- `Windows`, `Linux` MyOffice Mail
- `Windows`, `Linux` R7-Office Organizer
- `macOS` Apple Mail
- `macOS` Canary Mail
- `macOS` Spark
- `macOS` Mimestream
- `macOS` Airmail
- `macOS` Post Box
- `macOS` Boxy Suite 2
- `macOS` Twobird
- `macOS` Shift
- `macOS` Clean Email
- `macOS` eM Client
- `macOS` Superhuman
- `macOS` Polymail
- `macOS` HEY
- `macOS` Mail+ for Gmail
- `macOS` Spike mail

`Windows` Der Schutz vor E-Mail-Bedrohungen kann möglicherweise nicht immer auf Protokollebene auf Nachrichten zugreifen (z. B. bei Verwendung der Microsoft Exchange-Lösung). Aus diesem Grund umfasst Mail-Anti-Virus die Erweiterung „Kaspersky ASAP Outlook Plugin“ für Microsoft Office Outlook. Mit dieser Erweiterung können Nachrichten auf der Ebene des E-Mail-Clients untersucht werden. Das Kaspersky ASAP Outlook-Plug-in unterstützt Vorgänge mit Outlook 2010, 2013, 2016, 2019 und 2021.

Wenn ein Mail-Client in einem Browser geöffnet ist, untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ die Nachrichten nicht.

Wenn in einer Anlage eine schädliche Datei gefunden wird, fügt Kaspersky Endpoint Security dem Nachrichtenbetreff Informationen über die ausgeführte Aktion hinzu, z. B. *[Die Nachricht wurde verarbeitet.] <Nachrichtenbetreff>*.

Einstellungen für Mail-Anti-Virus

Einstellungen	Betriebssystem	Beschreibung
Untersuchungsausnahmen	`Windows` `macOS` `Linux`	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. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.
Aktion beim Fund einer Bedrohung	`Windows` `macOS` `Linux`	**Desinfizieren – Löschen, wenn Desinfektion fehlschlägt**. Wird in einer ein- oder ausgehenden Nachricht ein infiziertes Objekt gefunden, versucht das Programm, das gefundene 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>*. `Windows` `Linux` **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. Wird in einer ausgehenden Nachricht ein infiziertes Objekt gefunden, versucht das Programm, das gefundene Objekt zu desinfizieren. Wenn das Objekt nicht desinfiziert werden kann, blockiert das Programm das Senden der Nachricht, und der Mail-Client meldet einen Fehler. **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. `Linux` Für Linux-Geräte versucht die Komponente „Schutz vor E-Mail-Bedrohungen“ nicht, ein infiziertes Objekt in ausgehenden Nachrichten zu desinfizieren, sondern blockiert sofort die Übertragung der Nachricht.
POP3-, SMTP-, NNTP- und IMAP-Datenverkehr untersuchen	`Windows`	Untersuchung des Datenverkehrs, der über die Protokolle POP3, SMTP, NNTP und IMAP übertragen wird, durch die Komponente „Schutz vor E-Mail-Bedrohungen“.
Erweiterung für Microsoft Outlook verbinden	`Windows`	Wenn das Kontrollkästchen aktiviert ist, ist die Untersuchung von E-Mail-Nachrichten, die mit den Protokollen POP3, SMTP, NNTP und IMAP übertragen werden, aktiviert. Die Untersuchung erfolgt durch die in Microsoft Outlook integrierte Erweiterung. Das Programm kann ein- und ausgehende Nachrichten von Microsoft Outlook in verschiedenen Phasen untersuchen: • **Beim Empfang untersuchen**. Wenn dieses Kontrollkästchen aktiviert ist, verwendet das Programm den Schutz vor E-Mail-Bedrohungen, wenn Nachrichten über Microsoft Outlook empfangen werden. • **Beim Lesen untersuchen**. • **Beim Senden untersuchen**. Erfolgt die E-Mail-Untersuchung mithilfe der Erweiterung für Microsoft Outlook, wird empfohlen, den Exchange-Cache-Modus zu verwenden. Ausführlichere Informationen über den Exchange-Cache-Modus und Tipps zu seiner Verwendung finden Sie in der Microsoft Knowledge Base.
Angehängte Archive untersuchen	`Windows` `Linux`	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	`Windows` `Linux`	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.

Einstellungen	Betriebssystem	Beschreibung
Archive nicht untersuchen, wenn größer als (MB)	`Windows` `macOS` `Linux`	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.)	`Windows` `macOS` `Linux`	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.
Anlagenfilterung	`Windows` `Linux`	Die Anlagenfilterung bestimmt die Aktion, die der Schutz vor E-Mail-Bedrohungen mit Dateien ausführt, die an E-Mail-Nachrichten angehängt sind. Die Anlagenfilterung funktioniert nicht für ausgehende E-Mail-Nachrichten. • **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. Die Dateitypen der Anhänge, die umbenannt oder aus der E-Mail-Nachricht entfernt werden sollen, können Sie in der Liste der Dateimasken angeben.

Schutz vor Web-Bedrohungen

Für Windows, macOS und Linux

Die Komponente „Schutz vor Web-Bedrohungen“ verhindert den Download schädlicher Dateien aus dem Internet und blockiert schädliche Websites und Phishing-Websites. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der heuristischen Analyse.

Die Komponente „Schutz vor Web-Bedrohungen“ untersucht den eingehenden HTTP-, HTTPS- und FTP-Datenverkehr sowie Websites und IP-Adressen.

`Linux` Schutz vor Web-Bedrohungen für ist standardmäßig deaktiviert. Das Aktivieren von Web Anti-Virus kann die Leistung installierter Drittanbieter-Anwendungen und des Betriebssystems verringern. Wie Sie das Programm konfigurieren, um Web Anti-Virus auf Linux-Geräten zu aktivieren, erfahren Sie in der Wissensdatenbank des Technischen Supports.

Einstellungen für Web Anti-Virus

Einstellungen	Betriebssystem	Beschreibung
Vertrauenswürdige Webadressen	`Windows` `macOS` `Linux`	Liste mit Webadressen, die der 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 für vertrauenswürdige Adressen kann beispielsweise verwendet werden, wenn die Komponente „Schutz vor Web-Bedrohungen“ den Download einer Datei von einer Ihnen bekannten Website verhindert. Sie können zur Liste der vertrauenswürdigen Webadressen entweder die konkrete Adresse einer Webseite/Website hinzufügen oder eine Adressmaske für eine Webseite/Website. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

Einstellungen	Betriebssystem	Beschreibung
Untersuchungsausnahmen	`Windows`	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. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.
Aktion beim Fund einer Bedrohung	`Windows` `macOS` `Linux`	**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. **Erlauben, informieren oder Aktion erfragen (je nach Betriebssystem)**. `Windows` Wenn diese Option ausgewählt ist und ein infiziertes Objekt im Web-Datenverkehr erkannt wird, erlaubt Kaspersky Endpoint Security den Download dieses Objekts auf den Computer, fügt jedoch Informationen über das infizierte Objekt zur Liste der aktiven Bedrohungen hinzu. `macOS` Kaspersky Endpoint Security zeigt eine Benachrichtigung mit Informationen über die Art der Malware an, mit der das Objekt im Web-Datenverkehr infiziert wurde, und fordert den Benutzer auf, die Aktion auszuwählen, die Kaspersky Endpoint Security für dieses Objekt ausführen soll. Die verfügbaren Aktionen können je nach Objektstatus variieren. `Linux` Kaspersky Endpoint Security informiert den Benutzer über den Fund eines infizierten Objekts im Web-Datenverkehr. Der Schutz vor Web-Bedrohungen erlaubt den Download dieses Objekts auf das Gerät. Dabei protokolliert die Anwendung die Informationen über das infizierte Objekt und fügt es zur Liste der aktiven Bedrohungen hinzu.

Schutz vor Netzwerkbedrohungen

Für Windows, macOS und Linux

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.

`Linux` Der Schutz vor Netzwerkbedrohungen ist standardmäßig deaktiviert. Wenn der Schutz vor Netzwerkbedrohungen aktiviert ist, kann die Leistung installierter Drittanbieter-Anwendungen und des Betriebssystems sinken. Wie Sie das Programm konfigurieren, um den Schutz vor Netzwerkbedrohungen auf Linux-Geräten zu aktivieren, erfahren Sie in der Wissensdatenbank des Technischen Supports.

Einstellungen für den Schutz vor Netzwerkbedrohungen

Einstellungen	Betriebssystem	Beschreibung
Vertrauenswürdige IP-Adressen	`Windows` `Linux`	Liste der IP-Adressen von vertrauenswürdigen Geräten. Die Netzwerkaktivität von diesen Adressen wird von der Komponente „Schutz vor Netzwerkbedrohungen" nicht blockiert. `Windows` Sie können eine IP-Adresse mit Angabe des Ports oder der Portbereiche und des Protokolls hinzufügen. `Linux` Sie können nur eine IP-Adresse zur Ausnahmeliste hinzufügen. Für Netzwerkangriffe von den IP-Adressen, die zur Ausnahmeliste gehören, nimmt das Programm keine Informationen in den Bericht auf.

Einstellungen	Betriebssystem	Beschreibung
Aktion beim Fund einer Bedrohung	`Windows` `macOS` `Linux`	**Blockieren**. Sobald eine Bedrohung erkannt wird, blockiert der Schutz vor Netzwerkbedrohungen den Angriff. **Angriff und angreifendes Gerät blockieren für (Min.)**. Ist diese Option aktiviert, so fügt die Komponente „Schutz vor Netzwerkbedrohungen" den angreifenden Computer zur Sperrliste hinzu. Das bedeutet, dass die Komponente „Schutz vor Netzwerkbedrohungen" die Netzwerkverbindung mit dem angreifenden Computer nach dem ersten Netzwerkangriffsversuch für die angegebene Zeitspanne blockiert. Diese Sperre schützt den Computer des Benutzers automatisch vor möglichen zukünftigen Netzwerkangriffen von derselben Adresse aus. Die minimale Zeit, für die ein angreifender Computer auf die Blockliste gesetzt werden kann, ist eine Minute. Die maximale Dauer beträgt 999 Minuten. Kaspersky Endpoint Security löscht die Sperrliste, wenn das Programm neu gestartet wird und wenn die Einstellungen für den „Schutz vor Netzwerkbedrohungen" geändert werden.
Port-Scanning und Netzwerk-Flooding als Angriffe betrachten	`Windows`	Bei Angriffen des Typs *Port Scanning* werden die UDP-Ports, TCP-Ports und Netzwerkdienste des Computers gescannt. Bei diesem Angriff können Angreifer ermitteln, wie anfällig der Computer für Angriffe ist, bevor sie gefährlichere Arten von Netzwerkangriffen starten. Mithilfe von Port Scanning können Angreifer außerdem das Betriebssystem des Computers identifizieren und die entsprechenden Netzwerkangriffe für dieses Betriebssystem auswählen. *Network Flooding* ist ein Angriff auf die Netzwerkressourcen eines Unternehmens (z. B. auf Webserver). Bei diesem Angriff wird eine große Anzahl von Anforderungen gesendet, was die Bandbreite der Netzwerkressourcen überlastet. In solchen Fällen können Benutzer nicht auf die Netzwerkressourcen des Unternehmens zugreifen. Wenn dieses Kontrollkästchen aktiviert ist, überwacht Kaspersky Endpoint Security den Netzwerkverkehr, um diese Angriffe zu erkennen. Wenn ein Angriff erkannt wird, benachrichtigt das Programm den Benutzer und sendet ein entsprechendes Ereignis an Kaspersky Security Center. Das Programm stellt Informationen über den angreifenden Computer bereit, die für eine rechtzeitige Reaktion auf Bedrohungen erforderlich sind. Sie können die Erkennung dieser Angriffstypen deaktivieren, falls einige Ihrer zulässigen Programme Vorgänge ausführen, die für diese Angriffstypen typisch sind. Auf diese Weise können Fehlalarme vermieden werden.
MAC-Spoofing-Schutz	`Windows`	Bei einem Angriff vom Typ *MAC-Spoofing* wird die MAC-Adresse eines Netzwerkgeräts (einer Netzwerkkarte) verändert. Dann kann der Angreifer die Daten, die an das Gerät gesendet werden, auf ein anderes Gerät umleiten und auf diese Daten zugreifen. Kaspersky Endpoint Security kann Mac-Spoofing-Angriffe blockieren und solche Angriffe melden

Firewall.

Für Windows, macOS und Linux

Die Komponente „Firewall" blockiert nicht autorisierte Verbindungen mit dem Computer, wenn das Internet oder ein lokales Netzwerk verwendet wird. Die „Firewall" kontrolliert auch die Netzwerkaktivität der Programme auf dem Computer. Dadurch wird das lokales Unternehmensnetzwerk vor dem Diebstahl persönlicher Daten und anderen Angriffen geschützt. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der *vordefinierten Netzwerkregeln*.

`Linux` Für Linux-Geräte verwendet die App die Komponente „Firewall-Management". Die Komponente verwaltet die Einstellungen und Regeln der Betriebssystem-Firewall.

Einstellungen	Betriebssystem	Beschreibung
Regeln für Netzwerkpakete	`Windows` `macOS` `Linux`	Tabelle der Netzwerkregeln für Pakete. Netzwerkregeln für Pakete werden verwendet, um Netzwerkpakete unabhängig von Programmen einzuschränken. Solche Regeln schränken den eingehenden und ausgehenden Netzwerkverkehr durch bestimmte Ports des gewählten Datenprotokolls ein. Die Tabelle enthält vordefinierte Netzwerkregeln für Pakete, die von Kaspersky zum optimalen Schutz des Netzwerkverkehrs für Computer mit Microsoft Windows- und Linux-Betriebssystemen empfohlen werden. Die Firewall legt für jede Netzwerkregel für Pakete eine bestimmte Ausführungspriorität fest. Die Firewall führt die Netzwerkregeln für Pakete in der Reihenfolge aus, in der sie auf der Liste der Netzwerkregeln für Pakete stehen (von oben nach unten). Die Firewall sucht eine passende Paket-Netzwerkregel, die zu der Netzwerkverbindung passt, und führt die entsprechende Aktion aus: Die Netzwerkaktivität wird entweder erlaubt oder blockiert. Die Firewall ignoriert alle weiteren Paket-Netzwerkregeln für diese Netzwerkverbindung. Netzwerkregeln für Pakete besitzen eine höhere Priorität als Netzwerkregeln für Programme.
Verfügbare Netzwerke	`Windows` `macOS` `Linux`	Diese Tabelle enthält Informationen über Netzwerkverbindungen, welche die Firewall auf dem Benutzercomputer gefunden hat. Dem Internet wird standardmäßig der Status **Öffentliches Netzwerk** zugewiesen. Der Typ des Internets kann nicht geändert werden. Die folgenden Netzwerkverbindungsarten sind verfügbar: • **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. Die Firewall filtert die Netzwerkaktivität für jedes Programm nach den für dieses Programm vorhandenen Netzwerkregeln. • **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.
Erlaubnisregeln für die Ports des Administrationsagenten immer hinzufügen	`macOS` `Linux`	Dieses Kontrollkästchen aktiviert oder deaktiviert das automatische Hinzufügen von Erlaubnisregeln für Ports des Administrationsagenten.
Programmrechte und geschützte Ressourcen	`Windows`	**Programm**. Tabelle der Programme, die von der Komponente „Firewall“ kontrolliert werden. Die Programme sind auf Sicherheitsgruppen verteilt. Die Sicherheitsgruppe entscheidet über die Rechte, die Kaspersky Endpoint Security zur Kontrolle der Netzwerkaktivität von Programmen verwendet. Sie können ein Programm aus einer Liste aller Programme auswählen, die auf den Computern installiert sind, für welche die Richtlinie gilt, und das Programm einer Sicherheitsgruppe zuweisen. **Netzwerkregeln**. Tabelle der Netzwerkregeln für Programme, die zu einer Sicherheitsgruppe gehören. Nach diesen Regeln reguliert die „Firewall“ die Netzwerkaktivität von Programmen. Die Tabelle enthält die vordefinierten Netzwerkregeln, die von den Kaspersky-Experten empfohlen werden. Diese Netzwerkregeln dienen dem optimalen Schutz des Netzwerkverkehrs. Die vordefinierten Netzwerkregeln können nicht gelöscht werden.

Sicherheitskontrolle

Gerätekontrolle

Für Windows, macOS und Linux

Die „Gerätekontrolle“ verwaltet den Zugriff von Benutzern auf die Geräte, die installiert oder mit dem Computer verbunden sind (z. B. auf Festplatten, Kamera oder WLAN-Modul). Bei einer Verbindung mit diesen Geräten kann der Computer so vor einer Infektion geschützt werden, und Datenverlust oder Datendiebstahl lassen sich verhindern.

Die Gerätekontrolle erlaubt oder blockiert den Zugriff auf Geräte auf den folgenden Ebenen:

- **Gerätetyp**. Beispielsweise Drucker, Wechseldatenträger, CD/DVD-Laufwerke.
- **Schnittstelle**. Mithilfe einer *Verbindungsschnittstelle* können Geräte mit einem Gerät verbunden werden (z. B. über USB oder FireWire). Wenn der Modus **Je nach Schnittstelle** für einen Gerätetyp ausgewählt ist, kontrolliert das Programm den Zugriff auf das Gerät und berücksichtigt dabei den Modus für die Verbindungsschnittstelle, an die das Gerät angeschlossen ist (z. B. USB).
- **Vertrauenswürdige Geräte**. *Vertrauenswürdige Geräte* sind Geräte, auf die die angegebenen Benutzer oder Benutzergruppen jederzeit vollständigen Zugriff haben.

  Sie können vertrauenswürdige Geräte mithilfe der folgenden Daten hinzufügen:

  - `Windows` `macOS` **Modell**. Jedes Gerät besitzt eine einmalige Hersteller-ID (engl. Vendor ID – VID) und eine Produkt-ID (engl. Product ID – PID). Diese IDs finden Sie mithilfe von Betriebssystem-Tools in den Eigenschaften des Gerätes. Vorlage für die Eingabe einer VID und PID: `VID_1234&PID_5678`. Es bietet sich an, Geräte mithilfe des Modells hinzuzufügen, wenn Sie in Ihrem Unternehmen Geräte eines bestimmten Modells verwenden. Dadurch können Sie alle Geräte dieses Modells hinzufügen.
  - **ID**. Jedes Gerät besitzt eine einmalige ID (engl. Hardware ID – 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.
  - `Windows` `macOS` **Geräte nach Modellmaske**. Wenn Sie mehrere Geräte mit ähnlichen VIDs oder PIDs verwenden (z. B. Geräte desselben Herstellers), 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. Zum Beispiel `VID_05AC&PID_*`.
  - **Geräte 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*`.

`Linux` Bei Linux-Geräten hängt die von der Komponente ausgeführte Aktion vom Modus zum Abfangen von Dateivorgängen ab, der im Abschnitt „Allgemeine Einstellungen“, Unterabschnitt Erkennungseinstellungen ausgewählt ist.

Einstellungen	Betriebssystem	Beschreibung
Vertrauenswürdige Geräte	`Windows` `macOS` `Linux`	Liste der vertrauenswürdigen Geräte und Benutzer, denen der Zugriff auf diese Geräte erlaubt ist. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.
Vorlagen für Nachrichten	`Windows` `Linux`	**Nachricht an den Benutzer**. Vorlage der Nachricht, die erscheint, wenn der Benutzer auf ein blockiertes Gerät zugreift. Diese Nachricht erscheint auch, wenn der Benutzer versucht, einen Vorgang mit dem Geräteinhalt auszuführen, zu dem dieser Benutzer nicht berechtigt ist. **Nachricht an den Administrator**. Vorlage für die Nachricht, die an den Administrator des lokalen Unternehmensnetzwerks gesendet wird, wenn die Zugriffsverweigerung auf ein Gerät oder das Verbot eines Vorgangs mit dem Geräteinhalt nach Meinung des Benutzers irrtümlicherweise erfolgt.
Anfragen auf temporären Zugriff erlauben	`Windows` `Linux`	Wenn das Kontrollkästchen aktiviert ist, ist die Schaltfläche **Zugriff erfragen** in der lokalen Programmoberfläche von Kaspersky Endpoint Security verfügbar. Mit dieser Schaltfläche kann der Benutzer den temporären Zugriff auf ein blockiertes Gerät erfragen.
Funktionsmodus	`Linux`	Kaspersky Endpoint Security führt die ausgewählte Aktion aus, wenn versucht wird, Zugriff auf ein Gerät zu erhalten, auf das der Zugriff gemäß den Gerätekontrolle-Einstellungen 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**. Wenn Sie diese Option auswählen, wendet Kaspersky Endpoint Security den für das Gerät oder die Schnittstelle angegebenen Zugriffsmodus an.
Geräte und WLAN-Netzwerke	`Windows` `macOS` `Linux`	Eine Liste aller verfügbaren Gerätetypen nach der Klassifikation der Komponente „Gerätekontrolle“, einschließlich der entsprechenden Varianten für den Zugriffsstatus.
Verbindungsschnittstellen	`Windows` `Linux`	Liste aller verfügbaren Schnittstellen nach der Klassifikation der Komponente „Gerätekontrolle“ und die entsprechenden Varianten für den Zugriffsstatus. Kaspersky Endpoint Security erlaubt oder verweigert den Zugriff auf Geräte je nach Art der Verbindungsschnittstelle, wenn der Modus **Von Verbindungsschnittstelle abhängig** ausgewählt ist.
Anti-Bridging	`Windows`	Anti-Bridging verhindert die Erstellung von Netzwerkbrücken und verhindert zu diesem Zweck, dass gleichzeitig mehrere Netzwerkverbindungen für den Computer hergestellt werden. Dadurch kann das Unternehmensnetzwerk vor Angriffen über ungeschützte und nicht autorisierte Netzwerke geschützt werden. Anti-Bridging blockiert die Herstellung mehrerer Verbindungen, wobei die Prioritäten der Geräte berücksichtigt werden. Je weiter oben ein Gerät auf der Liste steht, desto höher ist seine Priorität. Haben eine aktive Verbindung und eine neue Verbindung den gleichen Typ (z. B. WLAN), so blockiert Kaspersky Endpoint Security die aktive Verbindung und erlaubt die Herstellung der neuen Verbindung. Haben eine aktive Verbindung und eine neue Verbindung unterschiedliche Typen (z. B. Netzwerkadapter und WLAN), so blockiert Kaspersky Endpoint Security die Verbindung mit der niedrigeren Priorität und erlaubt die Herstellung der Verbindung mit der höheren Priorität. Anti-Bridging unterstützt die folgenden Gerätetypen: Netzwerkadapter, WLAN und Modem.

Web-Kontrolle

Für Windows, macOS und Linux

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.

Regeln für den Zugriff auf Websites

Die „Web-Kontrolle“ verwaltet den Zugriff von Benutzern auf Websites mithilfe von *Zugriffsregeln*. Sie können den Zugriff auf Websites für die folgenden Untersuchungsbereiche anpassen:

- **Kategorie der Website.** Eine Kategorisierung der Websites wird gewährleistet vom Cloud-Dienst für Kaspersky Security Network, von der heuristischen Analyse und von der Datenbank für unbekannte Websites (im Lieferumfang des Programms enthalten). Sie können den Benutzerzugriff auf bestimmte Kategorien beschränken, beispielsweise auf die Kategorie *Soziale Netzwerke* oder auf andere Kategorien.

- `Windows` **Datentyp**. Sie können für Benutzer den Zugriff auf bestimmte Daten auf einer Website beschränken und beispielsweise Bilder verbergen. Kaspersky Endpoint Security ermittelt den Datentyp aufgrund des Dateiformats, nicht nach der Erweiterung.

  Dateien in Archiven werden durch Kaspersky Endpoint Security nicht untersucht. Befinden sich beispielsweise Bilddateien in einem Archiv, so ermittelt Kaspersky Endpoint Security den Datentyp *Archive*, nicht *Bilddateien*.

- **Bestimmte Adresse**. Sie können eine Webadresse eingeben oder Masken verwenden.

Sie können gleichzeitig mehrere Methoden verwenden, um den Zugriff auf Websites zu regulieren. So können Sie z. B. den Zugriff auf den Datentyp *Dateien für Office-Programme* nur für die Website-Kategorie *Web-E-Mail* beschränken.

Mit der Web-Kontrolle können Sie zudem die folgenden erweiterten Einstellungen für Website-Zugriffsregeln konfigurieren:

- **Benutzer oder Gruppe, für den bzw. die die Regel der Programmkontrolle gelten soll**.

  Sie können beispielsweise den Internetzugriff über einen Browser für alle Unternehmensmitarbeiter beschränken, aber die IT-Abteilung ausnehmen.

- **Zeitplan für den Zugriff auf Geräte**.

  Sie können beispielsweise den Internetzugriff über einen Browser nur während der Arbeitszeit beschränken.

Einstellungen der Web-Kontrolle

Einstellungen	Betriebssystem	Beschreibung
Vorlagen für Nachrichten	`Windows` `Linux`	**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 beim Blockieren**. Das Eingabefeld enthält eine Vorlage für die Meldung, die erscheint, wenn eine Regel ausgelöst wird, die den Zugriff auf eine Webressource blockiert. **Nachricht an den Administrator**. Vorlage für die Nachricht, die an den Administrator des lokalen Unternehmensnetzwerks gesendet werden soll. Wird verwendet, wenn der Benutzer der Meinung ist, dass der Zugriff auf die Webressource irrtümlich blockiert wurde. Zum Verwalten der Nachrichtenvorlagen stehen spezielle Variablen zur Verfügung (z. B. `%USER_NAME%`). Wenn Sie Variablen verwenden, kann ein und dieselbe Nachrichtenvorlage für verschiedene Computer genutzt werden.
Regelliste	`Windows` `macOS` `Linux`	Liste der Zugriffsregeln für Webressourcen. Jede Regel besitzt eine Priorität. Je höher sich eine Regel in der Liste befindet, desto höher ist ihre Priorität. Wenn eine Website in mehreren Regeln vorkommt, reguliert die „Web-Kontrolle“ den Zugriff auf die Website nach der Regel mit der höchsten Priorität.

Einstellungen	Betriebssystem	Beschreibung
Standardmäßige Aktion	`Windows` `macOS` `Linux`	Die Regel für den Zugriff auf Webressourcen, für die keine anderen Regeln gelten. Folgende Optionen stehen zur Verfügung: • **Alle erlauben, die nicht in der Regelliste angegeben sind**. • **Alle blockieren, die nicht in der Regelliste angegeben sind**.
Aktive Browsersitzungen des Benutzers beenden, nachdem die Regel angewendet wurde	`Windows`	Wenn das Kontrollkästchen aktiviert ist, trennt die Web-Kontrolle die Verbindung zu blockierten Webressourcen sofort, nachdem die Richtlinie angewendet wurde. Der Browser bricht den Download von Daten von der Webseite sofort ab. Wenn Sie die Webseite aktualisieren oder zu einer anderen verbotenen Webseite wechseln, zeigt das Programm eine Warnung an. Die Web-Kontrolle ermöglicht das sofortige Trennen der Verbindung von Webressourcen nur in Webbrowsern. Für andere Programme schränkt die Web-Kontrolle neue Verbindungen nur ein. Wenn das Kontrollkästchen deaktiviert ist, beschränkt die Web-Kontrolle nur neue Verbindungen mit verbotenen Webressourcen. Aktive Verbindungen werden von der Web-Kontrolle nicht getrennt.
Überwachung von Websitzungen	`Windows`	Kaspersky Endpoint Security protokolliert Daten über den Besuch aller Websites, einschließlich erlaubter Websites. Kaspersky Endpoint Security sendet Ereignisse an Kaspersky Security Center, an das Windows-Ereignisprotokoll und an einen Bericht. Für die Überwachung der Internetaktivitäten des Benutzers müssen die Einstellungen für die Ereignisspeicherung angepasst werden. Browser, die die Überwachungsfunktion unterstützen: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. In anderen Browsern funktioniert die Überwachung der Benutzeraktivität nicht. Die Überwachung der Internetaktivitäten des Benutzers kann bei einer Entschlüsselung des HTTPS-Datenverkehrs mehr Computer-Ressourcen erfordern.

Programmkontrolle

Für Windows und Linux

Die „Programmkontrolle“ verwaltet den Start von Programmen auf den Benutzercomputern. Dadurch wird ermöglicht, die Sicherheitsrichtlinie des Unternehmens bei der Verwendung von Programmen zu erfüllen. Außerdem reduziert die „Programmkontrolle“ das Risiko einer Infektion des Computers. Dazu wird der Zugriff auf Programme beschränkt.

Die Komponente „Programmkontrolle“ verwendet Regeln, um den Start von Programmen auf geschützten Geräten zu überwachen. Eine Regel enthält Bedingungen und Aktionen, die die Komponente „Programmkontrolle“ ausführt, wenn eine Regel ausgelöst wird. Beispielsweise die Kategorie, zu der ein Programm gehört. Eine *Programmkategorie* ist eine Gruppe von Programmen, die gemeinsame Eigenschaften haben. Beispiele: Eine Kategorie für die ausführbare Dateien von installierten Programmen, oder eine Kategorie für die Programme, die in einem Unternehmen standardmäßig eingesetzt werden. Eine Kategorie kann jeweils nur in einer einzigen Regel verwendet werden.

Der Administrator kann eine Vielzahl von Regeln erstellen. Ein Programm kann die Kriterien mehrerer Regeln erfüllen. Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel. Kaspersky Endpoint Security überprüft bei jedem Programmstart, ob ein Programm mit einer Regel übereinstimmt. Kaspersky Endpoint Security vergleicht das Programm nacheinander mit allen Regeln der Programmkontrolle.

Einstellungen	Betriebssystem	Beschreibung
Vorlagen für Nachrichten	`Windows`	**Nachricht an den Benutzer**. Vorlage der Nachricht, die beim Auslösen einer Regel der Programmkontrolle erscheint, wenn diese Regel den Programmstart blockiert. **Nachricht an den Administrator**. Vorlage für die Nachricht, die an den Administrator des lokalen Unternehmensnetzwerks gesendet wird, wenn ein Programm nach Meinung des Benutzers irrtümlich blockiert wurde.
Funktionsmodus	`Windows` `Linux`	Sie können zwischen folgenden Varianten wählen: • **Alle erlauben, die nicht in der Regelliste angegeben sind**. Wenn diese Option ausgewählt ist, erlaubt die Programmkontrolle allen Benutzern den Start beliebiger Programme. Ausnahme: Programme, die durch Sperr-Regeln der Programmkontrolle verboten sind. • **Alle blockieren, die nicht in der Regelliste angegeben sind**. Wenn diese Option ausgewählt ist, verbietet die Programmkontrolle allen Benutzern den Start beliebiger Programme. Ausnahme: Programme, die durch Erlaubnisregeln der Programmkontrolle zugelassen sind.
Aktion beim Starten von Programmen	`Windows` `Linux`	• **Regeln anwenden**. Kaspersky Endpoint Security verwaltet den Programmstart gemäß dem ausgewählten Modus. • **Informieren**. Kaspersky Endpoint Security informiert darüber, wenn versucht wird, ein Programm zu starten.
Richtlinienregeln zu lokalen Regeln hinzufügen	`Linux`	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.
Strenge Überprüfung für digitale Signaturen verwenden	`Windows`	Sie können ein Zertifikat als Auslösebedingung für eine Regel der Programmkontrolle auswählen. Wenn dieses Kontrollkästchen aktiviert ist, wendet Kaspersky Endpoint Security Regeln nur auf die Programme an, die mit Zertifikaten aus dem vertrauenswürdigen Zertifikatspeicher des Systems signiert sind. Programme, die mit einem solchen Zertifikat signiert sind, werden auch von den Schutzkomponenten als vertrauenswürdig eingestuft, z. B. von der Aufgabe *Schadsoftware-Untersuchung*. Wenn Sie in einer Regel der Programmkontrolle jedoch ein Zertifikat aus einem anderen Speicher angeben, wendet Kaspersky Endpoint Security diese Regel nicht an. Wenn das Kontrollkästchen deaktiviert ist, wendet Kaspersky Endpoint Security Regeln auf die Programme an, die mit einem Zertifikat aus dem Windows-Speicher für vertrauenswürdige Stammzertifikate signiert sind. Solche Programme gehören nicht zur vertrauenswürdigen Zone. Die Schutzkomponenten überwachen die Aktivität solcher Programme.
Laden von DLL-Modulen überwachen	`Windows`	Ist das Kontrollkästchen aktiviert, so kontrolliert Kaspersky Endpoint Security das Laden von DLL-Modulen, wenn Programme von Benutzern gestartet werden. Informationen über das DLL-Modul und das Programm, das dieses DLL-Modul geladen hat, werden protokolliert. Wenn die Funktion zur Kontrolle des Ladens von DLL-Modulen und Treibern aktiviert ist, vergewissern Sie sich, dass in den „Programmkontrolle"-Einstellungen entweder die Regel **Goldene Kategorie** aktiviert ist oder eine andere Regel, welche die KL-Kategorie „**Goldene Kategorie\Vertrauenswürdige Zertifikate**" enthält und das Laden von DLL-Modulen und Treibern vor dem Start von Kaspersky Endpoint Security gewährleistet. Wenn die Kontrolle von DLL-Modulen und Treibern gleichzeitig mit der Regel **Goldene Kategorie** aktiviert ist, kann es zur Instabilität des Betriebssystems kommen. Kaspersky Endpoint Security kontrolliert nur jene DLL-Module und Treiber, die geladen wurden, nachdem das Kontrollkästchen aktiviert wurde. Nach dem Aktivieren des Kontrollkästchens wird empfohlen, den Computer neu zu starten, um sicherzustellen, dass das Programm alle DLL-Module und Treiber überwacht, einschließlich derer, die vor dem Start von Kaspersky Endpoint Security geladen wurden.
Regeln	`Windows` `Linux`	Regeln der Programmkontrolle, die Kaspersky Endpoint Security verwendet, um den Start von Programmen auf geschützten Geräten zu überwachen. Für jeden Modus der Programmkontrolle können Sie maximal 5 Regeln hinzufügen.
Vertrauenswürdige Programme mit Update-Funktionen	`Windows`	Ist das Kontrollkästchen aktiviert, so betrachtet Kaspersky Endpoint Security die Programme, welche unter die Regel fallen, als vertrauenswürdige Programme mit Update-Funktionen. Kaspersky Endpoint Security erlaubt solchen Programmen, neue ausführbare Dateien das zu erstellen und auszuführen.

Überwachung der System-Integrität

Für Windows und Linux

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist.

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. Die Überwachung der Systemintegrität kann im Echtzeitmodus ausgeführt werden und die Systemintegrität auch auf Befehl überprüfen.

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.

`Linux` Aufgrund der technischen Beschränkungen des Betriebssystems Linux kann das Programm nicht erkennen, welcher Benutzer oder Prozess die Änderungen an der Datei vorgenommen hat.

Einstellungen der Komponente "Überwachung der Systemintegrität"

Einstellungen	Betriebssystem	Beschreibung
Echtzeitüberwachung der Systemintegrität	`Windows`	Im Echtzeitmodus überwacht die Überwachung der Systemintegrität die Änderungen an Objekten, die Sie im Gültigkeitsbereich der Komponente (*Überwachungsbereich)* aufgenommen haben. Mit der Überwachung der Systemintegrität kann auch der unbefugte Zugriff auf solche Objekte in Echtzeit gesperrt werden.
Aktion bei Erkennung einer Systemänderung	`Windows`	**Regeln anwenden**. In diesem Modus blockiert die Überwachung der Systemintegrität Aktionen, die mit Dateien und Registrierungsschlüsseln aus dem Überwachungsbereich erfolgen, und generiert ein entsprechendes Ereignis. **Regeln testen (Informieren)**. In diesem Modus erlaubt die Überwachung der Systemintegrität Aktionen, die mit Dateien und Registrierungsschlüsseln aus dem Überwachungsbereich erfolgen, und generiert ein entsprechendes Ereignis.
Dateien und Registrierung überwachen	`Windows`	Die Überwachung der Systemintegrität überwacht Änderungen an Dateien, Ordnern und der Registrierung.
Geräte überwachen	`Windows`	Die Überwachung der Systemintegrität überwacht das Verbinden und Trennen externer Geräte.
Prüfung der Systemintegrität	`Windows`	Die Aufgabe zur Prüfung der Systemintegrität auf Befehl können Sie manuell oder nach einem Zeitplan ausführen. Um die Aufgabe *Prüfung der Systemintegrität* auszuführen, müssen Sie den Bereich der Komponente (*Überwachungsbereich*) anpassen und eine Baseline erstellen. Eine *Baseline* ist ein aufgezeichneter Zustand von Objekten im System, den die App beim Vergleich mit dem aktuellen Zustand als Referenz verwendet.
Überwachungsbereiche	`Linux`	Die Tabelle enthält die Überwachungsbereiche der Komponente „Überwachung der Systemintegrität“. Die App untersucht Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig enthält die Tabelle den Überwachungsbereich **Interne Kaspersky-Objekte**.
Ausschlussbereiche	`Linux`	Die Tabelle enthält Bereiche mit Ausschlüsse von der Untersuchung. Die Anwendung untersucht keine Dateien und Verzeichnisse an den in der Tabelle angegebenen Pfaden. Standardmäßig ist die Tabelle leer.
Ausnahmen nach Maske	`Linux`	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.

Vertrauenswürdige Zone

Für Windows, macOS und Linux

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.

In Kaspersky Endpoint Security können Datei- oder Ordnernamen durch Masken angegeben werden. Für Masken sind die folgenden Platzhalterzeichen zulässig:

- Zeichen `*`, das als Platzhalter für eine beliebige Zeichenkombination steht, die auch leer sein kann. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\*\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung txt, die sich in Ordnern auf Laufwerk C befinden, allerdings nicht in untergeordneten Ordnern.

- Zeichen `?`, das als Platzhalter für ein beliebiges Einzelzeichen steht. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\Folder\???.txt` umfasst die Pfade aller Dateien, die im Ordner mit dem Namen `Folder` enthalten sind, die Erweiterung TXT haben und deren Name aus drei Zeichen besteht.

Einstellungen der vertrauenswürdigen Zone

Einstellungen	Betriebssystem	Beschreibung
Webadressen	`Windows` `macOS` `Linux`	Liste mit Webadressen, die der 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 für vertrauenswürdige Adressen kann beispielsweise verwendet werden, wenn die Komponente „Schutz vor Web-Bedrohungen“ den Download einer Datei von einer Ihnen bekannten Website verhindert. Sie können zur Liste der vertrauenswürdigen Webadressen entweder die konkrete Adresse einer Webseite/Website hinzufügen oder eine Adressmaske für eine Webseite/Website.
IP-Adressen	`Windows` `Linux`	Liste der IP-Adressen von vertrauenswürdigen Geräten. Die Netzwerkaktivität von diesen Adressen wird von der Komponente „Schutz vor Netzwerkbedrohungen“ nicht blockiert. `Windows` Sie können eine IP-Adresse mit Angabe des Ports oder der Portbereiche und des Protokolls hinzufügen. `Linux` Sie können nur eine IP-Adresse zur Ausnahmeliste hinzufügen. Für Netzwerkangriffe von den IP-Adressen, die zur Ausnahmeliste gehören, nimmt das Programm keine Informationen in den Bericht auf.
Netzwerkports	`Windows` `macOS` `Linux`	Liste der bekannten und registrierten Ports, auf denen Datenströme durch die folgenden Komponenten überwacht werden: Web-Kontrolle, Schutz vor bedrohlichen Dateien, Schutz vor Web-Bedrohungen, Schutz vor E-Mail-Bedrohungen, Exploit-Prävention und Verhaltensanalyse. Wenn dieser Schalter aktiviert ist, wird der Port als vertrauenswürdig betrachtet und Daten, die auf Benutzergeräten über einen solchen Port laufen, werden nicht überwacht.
Vertrauenswürdige Zertifikate	`Windows` `macOS` `Linux`	Liste der Stammzertifikate, die Kaspersky Endpoint Security als vertrauenswürdig einstuft. Die Liste der vertrauenswürdigen Stammzertifikate wird bei der Untersuchung verschlüsselter Verbindungen verwendet.
Namen/IP-Adressen von vertrauenswürdigen Computern	`Windows`	Liste mit Host-Namen und IP-Adressen, die von der Komponente „Verhaltensanalyse“ als vertrauenswürdig eingestuft werden. Kaspersky Endpoint Security untersucht die angegebenen Geräte nicht auf Viren und andere bedrohliche Programme.

Einstellungen	Betriebssystem	Beschreibung
Domänen	`Windows` `Linux`	Liste der vertrauenswürdigen Domänen. Verschlüsselte Verbindungen mit diesen Domänen werden von den folgenden Komponenten nicht überwacht: Schutz vor Web-Bedrohungen, Web-Kontrolle und Cloud Discovery (nur für Windows-Geräte). Verbindungen mit diesen Domänen werden auf Windows-Geräten blockiert, wenn der Zugriff mittels SSL/TLS erfolgt und die Option „SSL/TLS-Verbindungen blockieren“ aktiviert ist.
Vertrauenswürdige Mount-Points	`Linux`	Liste der vertrauenswürdigen Mount-Points. Diese werden durch die folgenden Komponenten von der Untersuchung ausgeschlossen: Schutz vor bedrohlichen Dateien, Schutz vor Verschlüsselung, Programmkontrolle und Verhaltensanalyse. Die Mountpunkte müssen genau so angegeben werden, wie sie in der Ausgabe des Befehls `mount` angezeigt werden.
Ausnahmen für das Abfangen des Datenverkehrs	`Linux`	Liste der Netzwerkverbindungen, die Kaspersky Endpoint Security von der Überwachung des Datenverkehrs ausschließt. Ausnahmen für das Abfangen des Datenverkehrs wirken sich auf die folgenden Komponenten aus: Schutz vor Web-Bedrohungen, Schutz vor Netzwerkbedrohungen und Web-Kontrolle. Die ausgeschlossene Verbindung wird durch die folgenden Parameter definiert: • Richtung des Datenverkehrs, ein- oder ausgehend. • IP-Adresse des Remote-Geräts, d. h. die IP-Adresse, deren ein- und ausgehender Datenverkehr vom Abfangen ausgeschlossen wird (abhängig von der Richtung des Datenverkehrs). • Zielport, d. h. ein Port auf dem geschützten Gerät (bei einer Ausnahme für das Abfangen von eingehendem Datenverkehr) oder ein Port auf dem Remote-Gerät (bei einer Ausnahme für das Abfangen von ausgehendem Datenverkehr). Ausnahmen für das Abfangen des Datenverkehrs gelten nur für TCP-Verbindungen und haben keinen Einfluss auf Regeln für Netzwerkpakete.
WLAN-Netzwerke	`macOS`	Liste der vertrauenswürdigen WLAN-Netzwerke. Sie können die folgenden Einstellungen angeben: • Name des WLAN-Netzwerks. • Verschlüsselungstyp. • Authentifizierungstyp.
Programme	`Windows` `macOS` `Linux`	Die *Liste der vertrauenswürdigen Programme* ist eine Liste mit Programmen, deren Datei- oder Netzwerkaktivität nicht von Kaspersky Endpoint Security überwacht wird (selbst wenn diese schädlich ist). Gleiches gilt für den Zugriff dieser Programme auf die Systemregistrierung. Kaspersky Endpoint Security überwacht standardmäßig alle Objekte, die von einem beliebigen Programmprozess geöffnet, gestartet oder gespeichert werden, und kontrolliert die Aktivität aller Programme sowie den von diesen generierten Netzwerkverkehr. Nachdem eine Programm zur Liste der vertrauenswürdigen Programme hinzugefügt wurde, beendet Kaspersky Endpoint Security die Überwachung der Programmaktivitäten.
Ausnahmen für die Schadsoftware-Untersuchung	`Windows` `macOS` `Linux`	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.
Geräte	`Windows` `Linux`	*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.

Allgemeine Einstellungen

Konfiguration der Erkennung

Für Windows, macOS und Linux

Dieser Abschnitt beschreibt, wie Sie die Erkennungseinstellungen an Ihre Anforderungen anpassen können. Die Effektivität der Erkennung und Prävention von Bedrohungen hängt von der richtigen Konfiguration der Einstellungen ab.

Konfiguration der Erkennung

Einstellungen	Betriebssystem	Beschreibung
Erkennung anderer Objekttypen	`Windows` `macOS` `Linux`	Kaspersky Endpoint Security sucht unabhängig von den festgelegten Einstellungen stets nach Viren, Würmern, Trojanern und schädlichen Tools und blockiert diese. Diese Programme können dem Computer erheblichen Schaden zufügen. Zusätzlich können Sie die Erkennung der folgenden Objekttypen aktivieren: • **Legitime Software, mit der Angreifer den Computer oder die Benutzerdaten beschädigen 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. • `Windows` **Adware**. Sie zeigen auf der Oberfläche anderer Programme Werbebanner an oder leiten Suchanfragen auf Webseiten mit Werbung um. • `Windows` **Dialer**. Dialer können über ein Modem heimlich Telefonverbindungen herstellen. Dazu zählen auch legitime Programme, mit denen Hacker das Gerät oder die Benutzerdaten kompromittieren können. • `Windows` **Packer**. Damit Antiviren-Programme die Schadsoftware nicht erkennen, verpacken Hacker sie mithilfe spezieller Packer. Die Kaspersky-Experten haben analysiert, welche Packer am häufigsten von Angreifern eingesetzt werden.
Technologie zur Aktiven Desinfektion	`Windows`	Erkannte Schadsoftware wird in der Regel durch Kaspersky Endpoint Security entfernt, bevor der Computer infiziert werden kann. Die Technologie zur aktiven Desinfektion schützt den Computer vor aktiver Schadsoftware (vor aktiven Infektionen) und minimiert das Risiko eines Datenverlusts und der Ausbreitung einer Bedrohung. Wenn diese Technologie aktiviert ist, zeigt Kaspersky Endpoint Security beim Fund schädlicher Aktivitäten eine Pop-up-Benachrichtigung an. In der Benachrichtigung schlägt Kaspersky Endpoint Security die Option zur Ausführung der aktiven Desinfektion des Computers vor. Wenn der Benutzer zustimmt, neutralisiert Kaspersky Endpoint Security die Bedrohung und startet den Computer anschließend neu. Die Anwendung der Technologie zur aktiven Desinfektion beansprucht erhebliche Ressourcen des Computers, wodurch die Ausführung anderer Programme verlangsamt werden kann. Wenn das Programm gerade dabei ist, eine Infektion zu erkennen, kann es passieren, dass einige Betriebssystemfunktionen nicht verfügbar sind. Die Verfügbarkeit des Betriebssystems wird wiederhergestellt, wenn die „Aktive Desinfektion“ abgeschlossen ist und der Computer neu gestartet wird. Wenn Kaspersky Endpoint Security auf einem Computer mit Windows für Server installiert ist, zeigt Kaspersky Endpoint Security keine Benachrichtigung an. Deshalb können Sie keine Aktion zur Desinfektion einer aktiven Bedrohung auswählen. Um eine Bedrohung zu desinfizieren, müssen Sie die Technologie der Aktiven Desinfektion aktivieren – in den Programmeinstellungen – und die Aktive Desinfektion sofort ausführen – in den Aufgabeneinstellungen der *Schadsoftware-Untersuchung*. Anschließend müssen Sie die Aufgabe *Schadsoftware-Untersuchung* starten.
Zugriff auf Dateien während der Untersuchung blockieren	`Linux`	Wenn dieses Kontrollkästchen aktiviert ist, blockiert das Programm den Zugriff auf Dateien, während diese durch die Komponenten Schutz vor bedrohlichen Dateien und Gerätekontrolle, die Aktion Ausführungsprävention und die Aufgabe Untersuchung von Wechseldatenträgern untersucht werden. Wenn das Kontrollkästchen deaktiviert ist, ist der Zugriff auf jede Datei während der Untersuchung zulässig und die Untersuchung wird im asynchronen Modus durchgeführt.

Einstellungen	Betriebssystem	Beschreibung
Protokollierungseinstellungen für Objekte	`Linux`	**Virenfreie Objekte protokollieren**. Wenn das Kontrollkästchen aktiviert ist, protokolliert die Anwendung das Ereignis *ObjectProcessed* für jedes untersuchte Objekt. **Unverarbeitete Objekte protokollieren**. Wenn das Kontrollkästchen aktiviert ist, protokolliert das Programm das Ereignis *ObjectNotProcessed*. **Gepackte Objekte protokollieren**. Wenn das Kontrollkästchen aktiviert ist, protokolliert die App das Ereignis *PackedObjectDetected*.

Kaspersky Security Network

Für Windows, macOS und Linux

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_<Sprach-ID>.txt mit dem Text der Vereinbarung über Kaspersky Security Network ist im Lieferumfang des Programms enthalten.

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.

Einstellungen für Kaspersky Security Network

Einstellungen	Betriebssystem	Beschreibung
Erweiterten KSN-Modus verwenden	`Windows` `macOS` `Linux`	Im *Erweiterten KSN-Modus* sendet Kaspersky Endpoint Security zusätzliche Daten an Kaspersky. Unabhängig vom Zustand des Schalters verwendet Kaspersky Endpoint Security KSN für die Erkennung von Bedrohungen. `Linux` Bei Linux-Geräten ist diese Option ausgeblendet, wenn die Lösung *Kaspersky Private Security Network (KPSN)* verwendet wird.
Cloud-Modus verwenden	`Windows` `macOS` `Linux`	*Cloud-Modus* – Modus des Programms, in dem Kaspersky Endpoint Security eine eingeschränkte Version der Antiviren-Datenbanken verwendet. Das Funktionieren des Programms mit einer eingeschränkten Version der Antiviren-Datenbanken wird durch Kaspersky Security Network gewährleistet. Mithilfe der eingeschränkten Version der Antiviren-Datenbanken kann die Auslastung des Computer-Arbeitsspeichers etwa um die Hälfte reduziert werden. 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. Wenn das Kontrollkästchen aktiviert ist, verwendet Kaspersky Endpoint Security eine eingeschränkte Version der Antiviren-Datenbanken. Dadurch werden die Betriebssystemressourcen geschont. Nachdem das Kontrollkästchen aktiviert wurde, lädt Kaspersky Endpoint Security beim nächsten Update eine eingeschränkte Version der Antiviren-Datenbanken herunter. Wenn das Kontrollkästchen deaktiviert ist, verwendet Kaspersky Endpoint Security die vollständige Version der Antiviren-Datenbanken. Nachdem das Kontrollkästchen deaktiviert wurde, lädt Kaspersky Endpoint Security beim nächsten Update die vollständige Version der Antiviren-Datenbanken herunter.
Computerstatus, wenn die KSN-Server nicht verfügbar sind	`Windows`	Mit den Elementen dieser Dropdown-Liste wird der Computerstatus in Kaspersky Security Center für den Fall festgelegt, dass die KSN-Server nicht verfügbar sind.
Administrationsserver als KSN-Proxyserver verwenden	`Windows` `macOS` `Linux`	Ist das Kontrollkästchen aktiviert, so verwendet Kaspersky Endpoint Security den Dienst KSN Proxy. Die Einstellungen für den Dienst KSN Proxy können Sie in den Eigenschaften des Administrationsservers anpassen.

Einstellungen	Betriebssystem	Beschreibung
Kaspersky Security Network-Server verwenden, wenn kein KSN-Proxyserver verfügbar	`Windows` `macOS` `Linux`	Wenn das Kontrollkästchen aktiviert ist, verwendet Kaspersky Endpoint Security KSN-Server, wenn der Dienst KSN-Proxy nicht verfügbar ist. Die KSN-Server können sich sowohl bei Kaspersky als auch bei Drittanbietern befinden (wenn Kaspersky Private Security Network verwendet wird).

Interaktion mit den Benutzern

Für Windows, macOS und Linux

Dieser Abschnitt beschreibt, wie Sie die Einstellungen der Programmoberfläche und die Einstellungen der Benutzerinteraktion anpassen können.

Einstellungen der Programmoberfläche

Einstellungen	Betriebssystem	Beschreibung
Kaspersky Endpoint Security beim Hochfahren des Computers starten (empfohlen)	`Windows` `macOS`	Wenn diese Funktionalität aktiviert ist, wird Kaspersky Endpoint Security nach dem Laden des Betriebssystems gestartet und schützt den Computer während der gesamten Sitzung. Wenn diese Funktionalität deaktiviert ist, wird Kaspersky Endpoint Security nach dem Hochfahren des Betriebssystems nicht automatisch gestartet. Der Benutzer muss das Programm manuell starten. Der Schutz des Computers ist deaktiviert, was ein Risiko für die Daten des Benutzers darstellt.
Programmsymbol anzeigen	`Windows` `macOS`	Auf dem Client-Computer befindet sich ein Programmsymbol im Benachrichtigungsbereich. Der Benutzer kann im Kontextmenü des Symbols Vorgänge mit Kaspersky Endpoint Security ausführen. Kaspersky Endpoint Security zeigt Benachrichtigungen über dem Programmsymbol an.
Programmoberfläche für Benutzer nicht anzeigen	`Windows` `macOS`	Wenn dieses Kontrollkästchen aktiviert ist, erlaubt Kaspersky Endpoint Security dem Benutzer nicht, das Programmhauptfenster zu öffnen, und die Programmoberfläche wird auf dem Remote-Computer ausgeblendet. Wenn dieses Kontrollkästchen deaktiviert ist, kann der Benutzer das Hauptfenster von Kaspersky Endpoint Security öffnen und die Programmoberfläche auf dem Remote-Computer verwenden.
Abschnitt „Aktivitätsmonitor für Programme“ ausblenden	`Windows`	Wenn dieses Kontrollkästchen aktiviert ist, ist die Schaltfläche **Aktivitätsmonitor für Programme** im Hauptfenster von Kaspersky Endpoint Security auf dem Client-Computer nicht verfügbar. Der *Aktivitätsmonitor für Programme* dient dazu, in Echtzeit Informationen über die Aktivität von Programmen auf einem Benutzercomputer anzuzeigen.
Updates lokal verwalten	`macOS`	Wenn dieses Kontrollkästchen aktiviert ist, kann der Benutzer die Updates für Kaspersky Endpoint Security lokal auf dem Remote-Computer verwalten. Wenn dieses Kontrollkästchen deaktiviert ist, können Sie die Updates für Kaspersky Endpoint Security auf dem Remote-Computer nur mithilfe des Plug-ins von Kaspersky Endpoint Security in Kaspersky Security Center verwalten.
Schlüssel lokal verwalten	`macOS`	Wenn dieses Kontrollkästchen aktiviert ist, kann der Benutzer die Schlüssel für Kaspersky Endpoint Security lokal auf dem Remote-Computer verwalten. Wenn dieses Kontrollkästchen deaktiviert ist, können Sie die Schlüssel für Kaspersky Endpoint Security auf einem Remote-Computer nur mithilfe des Plug-ins von Kaspersky Endpoint Security in Kaspersky Security Center verwalten.
Das Programm beenden	`macOS`	Wenn dieses Kontrollkästchen aktiviert ist, ist der Befehl **Beenden** im Kontextmenü des Programmsymbols vorhanden. Der Benutzer eines Remote-Computers kann Kaspersky Endpoint Security auf dem Remote-Computer beenden. Wenn dieses Kontrollkästchen deaktiviert ist, ist der Befehl **Beenden** nicht im Kontextmenü des Programmsymbols vorhanden. Der Benutzer eines Remote-Computers kann Kaspersky Endpoint Security auf dem Remote-Computer nicht beenden.

Einstellungen	Betriebssystem	Beschreibung
Auf lokale Aufgaben zugreifen	`Windows` `Linux`	Wenn das Kontrollkästchen aktiviert ist, werden die lokalen Aufgaben auf der lokalen Programmoberfläche von Kaspersky Endpoint Security angezeigt. Sofern die Richtlinie keine zusätzlichen Einschränkungen festlegt, kann der Benutzer Aufgaben anpassen und starten. Das Konfigurieren eines Ausführungszeitplan ist für den Benutzer jedoch weiterhin nicht verfügbar. Der Benutzer kann Aufgaben nur manuell ausführen. Ist dieses Kontrollkästchen deaktiviert, so können lokale Aufgaben nicht verwendet werden. In diesem Modus werden lokale Aufgaben nicht nach Zeitplan gestartet. Aufgaben können auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security nicht gestartet und geändert werden. Dies gilt auch bei Verwendung der Befehlszeile. Der Benutzer kann wie bisher die Untersuchung einer Datei oder eines Ordners starten und dazu den Punkt **Auf Viren untersuchen** im Kontextmenü der Datei oder des Ordners verwenden. Dabei wird die Untersuchungsaufgabe mit den Einstellungswerten ausgeführt, die standardmäßig für die Aufgabe zur benutzerdefinierten Untersuchung gelten.
Gruppenaufgaben anzeigen	`Windows`	Wenn das Kontrollkästchen aktiviert ist, werden Gruppenaufgaben auf der lokalen Programmoberfläche von Kaspersky Endpoint Security angezeigt. Der Benutzer kann auf der Benutzeroberfläche die komplette Aufgabenliste einsehen. Wenn das Kontrollkästchen deaktiviert ist, zeigt Kaspersky Endpoint Security eine leere Aufgabenliste an.
Gruppenaufgaben verwalten	`Windows` `Linux`	Wenn das Kontrollkästchen aktiviert ist, können Benutzer die in der Kaspersky Endpoint Security-Konsole vorhandenen Gruppenaufgaben starten und anhalten. Der Benutzer kann Aufgaben auf der Benutzeroberfläche oder auf der vereinfachten Programmoberfläche starten und anhalten. Wenn das Kontrollkästchen deaktiviert ist, gibt es zwei Möglichkeiten: Kaspersky Endpoint Security startet geplante Aufgaben automatisch, oder der Administrator startet die Aufgaben manuell über die Kaspersky Endpoint Security-Konsole.
Computerstatus	`Windows`	Einstellungen für die Anzeige von Statusvarianten der Client-Computer, auf denen das Programm Kaspersky Endpoint Security installiert ist. Diese Statusvarianten werden in „Web Console" angezeigt, wenn Fehler bei der Anwendung einer Richtlinie oder bei der Aufgabenausführung auftreten. Die folgenden Statusvarianten sind möglich: *OK*, *Warnung* und *Kritisch*.
Meldungen zum Programmstatus	`Windows`	Einstellungen für Benachrichtigungen über Programmereignisse in der Taskleiste. Aktivieren Sie die Kontrollkästchen für die Ereigniskategorien, für die im Infobereich der Taskleiste Benachrichtigungen angezeigt werden sollen. • **Aktive Bedrohungen**. • **Neustart des Computers ist erforderlich**. • **Probleme mit den Anti-Malware-Datenbanken**. • **Probleme mit der Sicherheitsstufe**. • **Lizenzprobleme**. • **Updates verfügbar**. Treten Ereignisse auf, die zu den ausgewählten Kategorien gehören, so ändert sich das Programmsymbol im Infobereich der Taskleiste je nach Priorität der Warnung in oder .
Meldungen zum Status der lokalen Anti-Malware-Datenbanken	`Windows`	Einstellungen für die Benachrichtigungen über veraltete Antiviren-Datenbanken, die vom Programm verwendet werden. Sie können festlegen, nach wie vielen Tagen Kaspersky Endpoint Security die Benachrichtigungen „Datenbanken sind veraltet" und „Datenbanken sind stark veraltet" an den Benutzer senden soll.
Einstellungen für den Programmstart	`Linux`	Einstellungen für den Programmstart: • **Maximale Anzahl an fehlgeschlagenen Versuchen, das Programm zu starten**. • **Maximale Wartezeit für den Programmstart (Min.)**. Der kesl-Prozess wird nach Ablauf der angegebenen Wartezeit neu gestartet.

Einstellungen	Betriebssystem	Beschreibung
Programm-Updates ohne Neustart installieren	`Windows`	Ein Upgrade der Anwendung ohne Neustart sorgt für einen unterbrechungsfreien Serverbetrieb, wenn die Anwendungsversion aktualisiert wird. Das Programm-Upgrade ohne Neustart hat die folgenden Einschränkungen: • Ein Programm-Upgrade ohne Neustart ist ab Version 11.10.0 möglich. Beim Upgrade älterer Programmversionen müssen Sie den Computer neu starten. • Eine Installation von Patches ohne Neustart ist ab Version 11.11.0 möglich. Um Patches für frühere Versionen der Anwendung zu installieren, ist möglicherweise ein Neustart des Computers erforderlich. • Das Programm-Upgrade ohne Neustart ist nicht verfügbar auf Computern mit aktivierter Datenverschlüsselung (Kaspersky-Verschlüsselung (FDE), BitLocker, Verschlüsselung von Dateien (FLE)). Um ein Programm-Upgrade auf Computern mit aktivierter Datenverschlüsselung durchzuführen, muss der Computer neu gestartet werden. • Für das App-Upgrade auf einer virtuellen Maschine ist ein Neustart erforderlich. Um die App auf einer virtuellen Maschine upzugraden, müssen Sie die virtuelle Maschine neu starten. Wenn nach dem Upgrade von Kaspersky Endpoint Security auf Version 11.10.0 oder höher kein Neustart erfolgt, sind zwei Versionen des Programms Kaspersky Endpoint Security auf dem Computer installiert. Entfernen Sie die frühere Programmversion nicht manuell. Die frühere Version wird beim Neustart des Computers automatisch entfernt. Der Standardwert des Parameters ist vom Typ des Betriebssystem abhängig. Wenn die App auf einer Workstation installiert ist, ist die Option zum App-Upgrade ohne Neustart deaktiviert. Wenn die App auf einem Server installiert ist, ist die Option zum App-Upgrade ohne Neustart aktiviert.
Kompatibilität mit Fernverwaltungsanwendungen	`Windows`	Sollte bei der Verwendung von Kaspersky Endpoint Security zusammen mit Fernverwaltungs-Tools (RAT) Probleme auftreten, können Sie den Kompatibilitätsmodus aktivieren. Die Probleme können auf Inkompatibilitäten der RATs mit der Funktion Sicherer Desktop der Anwendung zurückzuführen sein. Diese Funktionalität hat den Zweck, Aktionen zu bestätigen, die die Sicherheitsstufe des Computers möglicherweise verringern können. Mit dieser Funktionalität kann eine Anwendung einen Bestätigungsdialog anzeigen, der von anderen Prozessen isoliert ist. Diese Funktionalität nutzt erhöhte Rechte, um die Sicherheit der Anfrage zu verbessern. Dadurch wird sichergestellt, dass nur der Benutzer die Aktion bestätigen kann, nicht aber die Schadsoftware. Durch den RAT-Kompatibilitätsmodus kann das Sicherheitsniveau des Computers sinken. Deshalb raten wir davon ab, den Kompatibilitätsmodus zu aktivieren, wenn Kaspersky Endpoint Security keine Probleme mit Ihrem RAT verursacht. Die Funktion ist standardmäßig deaktiviert. Beispiel: Wenn Sie den Browser im RemoteApp-Modus verwenden, zeigt Kaspersky Endpoint Security beim Besuch einer Website mit einem nicht vertrauenswürdigen Zertifikat möglicherweise kein Bestätigungsfenster an, da RemoteApp die Programmfunktionalität „Sicherer Desktop“ nicht unterstützt. Dies kann dazu führen, dass der Browser nicht mehr reagiert. Damit der Browser im RemoteApp-Modus ordnungsgemäß funktioniert, müssen Sie den Kompatibilitätsmodus aktivieren. Sie können auch versuchen, den Kompatibilitätsmodus zu aktivieren, wenn bei der Verwendung anderer Drittanbieter-Anwendungen Probleme mit der Funktionalität „Sicherer Desktop“ auftreten.

Leistung

Für Windows, macOS und Linux

Die Leistungseinstellungen von Kaspersky Endpoint Security beziehen sich auf den Energieverbrauch und die Nutzung von Computerressourcen.

Einstellungen	Betriebssystem	Beschreibung
Ressourcen für andere Programme freigeben	`Windows`	Während der Computer untersucht wird, beansprucht Kaspersky Endpoint Security die Computerressourcen. Dadurch erhöht sich möglicherweise die Belastung des Prozessors und der Laufwerksubsysteme. Dadurch können andere Anwendungen verlangsamt werden. Um die Leistung zu optimieren, bietet Kaspersky Endpoint Security einen *Modus zur Bereitstellung von Ressourcen an andere Anwendungen*. In diesem Modus kann das Betriebssystem die Priorität der Threads für die Untersuchungsaufgaben von Kaspersky Endpoint Security senken, wenn der Prozessor stark ausgelastet ist. Dadurch können Betriebssystemressourcen auf andere Anwendungen umverteilt werden. Gleichzeitig wird den Untersuchungsaufgaben weniger Prozessorzeit zugewiesen. Dies hat zur Folge, dass Kaspersky Endpoint Security mehr Zeit benötigt, um den Computer zu untersuchen. Der Modus zur Freigabe von Ressourcen für andere Programme ist standardmäßig aktiviert.
Geplante Aufgaben bei Akkubetrieb aufschieben oder überspringen	`Windows` `macOS` `Linux`	Wenn diese Funktion aktiviert ist, wechselt Kaspersky Endpoint Security in den Energiesparmodus. `Windows` Kaspersky Endpoint Security wird geplante Aufgaben *verschieben*. Bei Bedarf können Sie die Untersuchungs- und Update-Aufgaben manuell starten. `macOS` `Linux` Kaspersky Endpoint Security *bricht* geplante Aufgaben ab. Bei Bedarf können Sie die Untersuchungs- und Update-Aufgaben manuell starten. Wenn der Energiesparmodus aktiviert ist und der Computer im Akkubetrieb läuft, werden die folgende Aufgaben auch dann nicht gestartet, wenn ein Startzeitplan vorhanden ist: • *Schadsoftware-Untersuchung* • *Update der Anti-Malware-Datenbanken* • *Prüfung der Anwendungsintegrität* • *IOC-Untersuchung*.
CPU-Auslastung für Untersuchungsaufgaben begrenzen	`Windows` `macOS` `Linux`	Um die Leistung von Kaspersky Endpoint Security zu optimieren, können Sie die CPU-Auslastung durch Untersuchungsaufgaben begrenzen. Je nach verwendetem Betriebssystem können die Aufgaben, für die die CPU-Auslastung begrenzt wird, variieren: • `Windows` `Linux` Schadsoftware-Untersuchung • `macOS` `Linux` Untersuchung wichtiger Bereiche • `Linux` Inventar • `Linux` Untersuchung von Containern Wenn diese Funktionalität aktiviert ist, nähert sich die durchschnittliche Belastung aller CPU-Kerne durch die Untersuchungsaufgabe dem angegebenen Wert.
Begrenzung der Speichernutzung für Untersuchungsaufgaben (MB)	`Linux`	Sie können die Begrenzung der Speichernutzung für Untersuchungsaufgaben anpassen (*Schadsoftware-Untersuchung*, *Untersuchung wichtiger Bereiche*, *Inventarisierung* und *Untersuchung von Containern*).
Ausnahmen für die Untersuchung des Prozess-Speichers konfigurieren	`Linux`	Sie können Untersuchungsausnahmen für den Prozess-Speicher konfigurieren. Der Arbeitsspeicher der angegebenen Prozesse wird von der Anwendung nicht untersucht. Geben Sie den Pfad der Prozesse an, die das Programm von der Untersuchung des Prozess-Speichers ausschließen soll. Bei der Angabe des Pfades können Masken verwendet werden. Standardmäßig ist die Liste leer.
Speichernutzung des Programms begrenzen	`Linux`	Sie können die Nutzung des residenten Speichers für das Programm begrenzen. Standardmäßig wird die Begrenzung automatisch festgelegt. **Methode zur Grenzwertberechnung**: • **Keine Begrenzung**. Wenn diese Option ausgewählt ist, wird die Verwendung des residenten Speichers nicht begrenzt. • **Exakten Wert angeben (%)**. • **Exakten Wert angeben (MB)**. • **Kleineren der beiden Werte anwenden (% oder MB)**. • **Größeren der beiden Werte anwenden (% oder MB)**. • **Automatisch begrenzen (empfohlen)**. Wenn diese Option ausgewählt ist, wird die Verwendung des residenten Speichers automatisch begrenzt.

Einstellungen	Betriebssystem	Beschreibung
Überwachung der Programmstabilität aktivieren	`Linux`	Sie können die Überwachung der Stabilität von Kaspersky Endpoint Security aktivieren oder deaktivieren. Diese Funktion verfolgt, wie oft das Programm unerwartet beendet wird, und informiert den Administrator bei instabiler Programmleistung. Wenn das Kontrollkästchen aktiviert ist, überwacht das Programm den Betrieb von Kaspersky Endpoint Security. Um die Einstellungen zu übernehmen, starten Sie das Programm neu. 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>*.

Netzwerkeinstellungen

Für Windows, macOS und Linux

Sie können den Proxyserver für die Internetverbindung konfigurieren, den Überwachungsmodus für Netzwerkports auswählen und die Untersuchung geschützter Verbindungen einrichten.

Netzwerkeinstellungen

Einstellungen	Betriebssystem	Description
Vertrauenswürdige Stammzertifikate	`Windows` `macOS` `Linux`	Liste der vertrauenswürdigen Stammzertifikate. 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. Um Zertifikate zum Systemzertifikatspeicher hinzuzufügen, können Sie Active Directory-Gruppenrichtlinien verwenden.
Proxyserver	`Windows` `macOS` `Linux`	Proxyserver-Einstellungen für den Internetzugriff durch die Benutzer von Client-Computern. Kaspersky Endpoint Security verwendet diese Einstellungen für bestimmte Schutzkomponenten und auch für das Update der Datenbanken und Programm-Module.
Proxyserver-Authentifizierung verwenden	`Windows` `macOS` `Linux`	Wenn dieses Kontrollkästchen aktiviert ist, verwendet das Programm bei der Verbindung mit dem Proxyserver die Authentifizierung mit Benutzername und Kennwort. `Windows` Für Windows-Geräte müssen Sie einen Authentifizierungstyp auswählen: • **NTLM-Authentifizierung**. NTLM-Authentifizierung mit dem aktuellen Benutzerkonto (Standard). • **NTLM-Authentifizierung mit Benutzername und Kennwort**. NTLM-Authentifizierung mit manuell angegebenen Anmeldedaten. • **Benutzername und Kennwort**. Authentifizierung mit manuell angegebenen Anmeldedaten. • **Automatische Authentifizierung**. • **Kerberos-Authentifizierung**. Kerberos-Authentifizierung mit dem aktuellen Benutzerkonto. • **Kerberos-Authentifizierung mit Benutzername und Kennwort**. Kerberos-Authentifizierung mit manuell angegebenen Anmeldedaten.
Einen Proxyserver für lokale Adressen umgehen	`Windows` `macOS`	Ist dieses Kontrollkästchen aktiviert, so verwendet Kaspersky Endpoint Security keinen Proxyserver, wenn ein Update aus einem gemeinsamen Ordner erfolgt.
Keinen Proxyserver für Komponenten verwenden	`Linux`	Aktivieren Sie die Kontrollkästchen neben den Programmkomponenten, für die der Proxyserver nicht verwendet werden soll: • **Endpoint Detection and Response Expert (on-premise)** – keinen Proxyserver verwenden, wenn eine Verbindung zu KATA-Servern hergestellt wird. • **KATA Sandbox** – keinen Proxyserver verwenden, wenn eine Verbindung zu Central Node-Servern hergestellt wird, die die Interaktion mit KATA Sandbox gewährleisten. • **Network Detection and Response (KATA)** – keinen Proxyserver verwenden, wenn eine Verbindung zu Network Detection and Response-Servern hergestellt wird.
Für die angegebenen IP-Adressen und DNS-Namen keinen Proxyserver verwenden	`Linux`	Die Tabelle enthält eine Liste mit IP-Adressen und DNS-Namen, für die der Proxyserver nicht verwendet werden soll. Für die Angabe der Adressen können Masken verwendet werden (Symbole `*` und `?`). In der Tabelle können Sie Adressen hinzufügen, bearbeiten oder löschen.

Einstellungen	Betriebssystem	Description
Untersuchung verschlüsselter Verbindungen	`Windows` `macOS` `Linux`	Diese Funktion ermöglicht es den Komponenten Schutz vor Web-Bedrohungen, Schutz vor E-Mail-Bedrohungen, Web-Kontrolle und Cloud Discovery, verschlüsselte Verbindungen (HTTPS) zu überwachen und zu verarbeiten. `Linux` Für Linux-Geräte ist die Option **Richtlinie zur Überprüfung von Zertifikaten** verfügbar, die festlegt, auf welche Weise das Programm Zertifikate überprüft: • **Lokale Überprüfung**: Das Programm überprüft Zertifikate, ohne das Internet zu verwenden. • **Vollständige Überprüfung** (Standard): Das Programm verwendet das Internet, um fehlende Ketten, die zur Überprüfung eines Zertifikats erforderlich sind, zu überprüfen und herunterzuladen.
Vertrauenswürdige Domänen	`Windows` `Linux`	Es wird eine Liste mit Webadressen verwendet, für die Kaspersky Endpoint Security keine Netzwerkverbindungen untersucht. In diesem Fall untersucht Kaspersky Endpoint Security den HTTPS-Datenverkehr vertrauenswürdiger Webadressen nicht, wenn die Komponenten „Schutz vor Web-Bedrohungen“, „Schutz vor E-Mail-Bedrohungen“ und „Web-Kontrolle“ aktiv sind. Sie können einen Domänennamen oder eine IP-Adresse eingeben. Kaspersky Endpoint Security unterstützt das Zeichen `*` für die Eingabe einer Maske in Domänennamen.
Datenverkehr bei getakteter Verbindung beschränken	`Windows`	Wenn dieses Kontrollkästchen aktiviert ist, beschränkt das Programm selbstständig den Netzwerkverkehr, wenn das Limit für die Verbindungskosten mit dem Internet erreicht wurde. Kaspersky Endpoint Security betrachtet eine Hochgeschwindigkeits-Internetverbindung als getaktet. Eine WLAN-Verbindung gilt als nicht getaktet. Cost-Aware Networking funktioniert auf Computern mit Windows 8 oder höher.
Skript zur Interaktion mit Webseiten in den Web-Datenverkehr einbinden	`Windows`	Wenn dieses Kontrollkästchen aktiviert ist, bindet Kaspersky Endpoint Security ein Skript in den Datenverkehr ein, das der Interaktion mit Webseiten dient. Dieses Skript stellt sicher, dass die Web-Kontrolle-Komponente korrekt arbeiten kann. Das Skript ermöglicht die Registrierung von Web-Kontrolle-Ereignissen. Kaspersky-Experten empfehlen, dieses Webseiten-Interaktionsskript in den Datenverkehr einzuspeisen, um den korrekten Betrieb der Web-Kontrolle zu gewährleisten.
Verschlüsselte Verbindungen mit Websites, die EV-Zertifikate verwenden, untersuchen	`Windows`	EV-Zertifikate (Extended Validation Certificate) bestätigen die Authentizität von Websites und erhöhen die Sicherheit der Verbindung. Die Browser informieren durch ein Schloss-Symbol in der Adressleiste darüber, ob eine Website ein EV-Zertifikat hat. Außerdem kann die Adressleiste des Browsers vollständig oder teilweise grüne Farbe besitzen. Wenn dieser Schalter aktiviert ist, werden geschützte Verbindungen, die ein EV-Zertifikat verwenden, vom Programm entschlüsselt und überwacht. Wenn der Schalter deaktiviert ist, hat Kaspersky Endpoint Security keinen Zugriff auf den Inhalt des HTTPS-Datenverkehrs. Deshalb kontrolliert das Programm den HTTPS-Datenverkehr nur anhand der Adresse einer Website, z. B. `https://bing.com`. Wenn Sie eine Website mit einem EV-Zertifikat zum ersten Mal öffnen, wird die verschlüsselte Verbindung unabhängig davon entschlüsselt, ob das Kontrollkästchen aktiviert ist oder nicht.
SSL 2.0-Verbindungen blockieren	`Windows`	Ist das Kontrollkästchen aktiviert, überwacht und blockiert das Programm die Netzwerkverbindungen, die über das SSL 2.0-Protokoll hergestellt werden. Ist das Kontrollkästchen deaktiviert, werden die Netzwerkverbindungen, die über das Protokoll SSL 2.0 hergestellt werden, nicht blockiert. Dabei überwacht das Programm den Netzwerkverkehr über dieses Protokoll nicht.
TLS 1.0-Verbindungen blockieren	`Windows`	Ist das Kontrollkästchen aktiviert, blockiert das Programm die Netzwerkverbindungen, die über das Protokoll TLS 1.0 hergestellt werden. Ist das Kontrollkästchen deaktiviert, werden die Netzwerkverbindungen, die über das Protokoll TLS 1.0 hergestellt werden, nicht blockiert. Das Programm überwacht den Netzwerkverkehr über dieses Protokoll. Alle Komponenten des Programms funktionieren ohne Einschränkungen.
SSL 3.0-Verbindungen blockieren	`Windows`	Ist das Kontrollkästchen aktiviert, blockiert das Programm die Netzwerkverbindungen, die über das Protokoll SSL 3.0 hergestellt werden. Ist das Kontrollkästchen deaktiviert, werden die Netzwerkverbindungen, die über das Protokoll SSL 3.0 hergestellt werden, nicht blockiert. Das Programm überwacht den Netzwerkverkehr über dieses Protokoll. Alle Komponenten des Programms funktionieren ohne Einschränkungen.

Einstellungen	Betriebssystem	Description
Überwachte Ports	`Windows` `macOS` `Linux`	**Alle Netzwerkports überwachen**. In diesem Modus für die Überwachung von Netzwerkports überwachen die Schutzkomponenten (Schutz vor bedrohlichen Dateien, Schutz vor Web-Bedrohungen und Schutz vor E-Mail-Bedrohungen) die Datenströme, die über beliebige offene Netzwerkports des Computers übertragen werden. **Nur ausgewählte Netzwerkports überwachen**. In diesem Überwachungsmodus für Netzwerkports kontrollieren die Schutzkomponenten die ausgewählten Ports des Computers und die Netzwerkaktivität der ausgewählten Programme. Eine Liste der Netzwerkports, über die E-Mail-Nachrichten und Netzwerkverkehr gewöhnlich übertragen werden, ist gemäß der Empfehlungen der Kaspersky-Experten vorgegeben. Bei Mac-Geräten können nur die ausgewählten Ports überwacht werden.
Überwachte Programme	`Windows`	Die Liste der Programme, für die der gesamte Datenverkehr auf allen Ports unabhängig von den Einstellungen für die Port-Untersuchung überwacht wird.
Zertifikatspeicher für Firefox auswählen	`macOS`	**System Roots-Schlüsselbund (empfohlen)**. Wenn diese Option ausgewählt ist, verwendet Kaspersky Endpoint Security ein Stammzertifikat aus dem Schlüsselbund „System Roots“, um den verschlüsselten HTTPS-Datenverkehr im Browser Mozilla Firefox zu untersuchen. Dieser Status gilt als Standard. **Zertifikatspeicher aus den Einstellungen von Mozilla Firefox**. Wenn diese Option ausgewählt ist, verwendet Kaspersky Endpoint Security das Zertifikat aus dem Zertifikatspeicher des Browsers. In diesem Fall müssen Sie das Kaspersky Endpoint Security-Zertifikat manuell zum Zertifikatspeicher von Mozilla Firefox hinzufügen. Weitere Informationen finden Sie im Artikel So fügen Sie das Kaspersky-Zertifikat zum Zertifikatspeicher von Mozilla Firefox hinzu.
Modus zum Abfangen des Datenverkehrs	`Linux`	**iptables**. Kaspersky Endpoint Security verwendet das Dienstprogramm iptables zum Abfangen des Datenverkehrs. **eBPF**. Das Programm verwendet die eBPF-Technologie, um den Datenverkehr abzufangen.

Container untersuchen

Für Linux

Die Anwendung untersucht gestartete Container und Namespaces in Echtzeit. Das Programm unterstützt die Integration in das Container-Management-System Docker, in die CRI-O-Umgebung sowie in die Dienstprogramme Podman und runc.

Für die Untersuchung von Containern muss die Komponente Schutz vor bedrohlichen Dateien aktiviert werden. Bei der Untersuchung von Containern und Namensräumen werden die Einstellungen des Schutzes vor bedrohlichen Dateien verwendet.

Die Anwendung prüft keine Namensräume und Container, es sei denn, auf dem Betriebssystem sind Komponenten für die Arbeit mit Containern und Namensräumen installiert.

Einstellungen der Untersuchung von Containern

Einstellungen	Betriebssystem	Beschreibung
Aktion beim Fund einer Bedrohung	`Linux`	**Container überspringen**. Wenn ein infiziertes Objekt erkannt wird, führt das Programm keine Aktionen mit dem Container durch. **Container anhalten**. Wenn ein infiziertes Objekt erkannt wird, hält das Programm den Container an. **Container anhalten, falls Desinfektion fehlschlägt**. Wenn ein infiziertes Objekt nicht desinfiziert werden konnte, hält das Programm den Container an.
Docker verwenden	`Linux`	Verwendung der Docker-Umgebung. Um die Umgebung zu verwenden, geben Sie einen Pfad oder die URI (universal resource ID) des Docker-Sockets ein.
CRI-O verwenden	`Linux`	Verwendung der CRI-O-Umgebung. Um diese Umgebung zu verwenden, geben Sie den Pfad der CRI-O-Konfigurationsdatei ein.

Einstellungen	Betriebssystem	Beschreibung
Podman verwenden	`Linux`	Verwendung des Podman-Tools. Um dieses Dienstprogramm zu verwenden, geben Sie den Pfad der ausführbaren Datei des Dienstprogramms und den Pfad zum Stammverzeichnis des Container-Speichers ein.
runc verwenden	`Linux`	Verwendung des runc-Tools. Um dieses Dienstprogramm zu verwenden, geben Sie den Pfad der ausführbaren Datei des Dienstprogramms und den Pfad zum Stammverzeichnis des Container-Statusspeichers ein.

Technischen Support

Für Windows und Linux

Zur Behebung potentieller Fehlfunktionen von Kaspersky Endpoint Security auf Computern benötigen die Mitarbeiter des Technischen Supports möglicherweise Informationen über das System und die Ereignisse, die während der Programmausführung aufgetreten sind. Diese Informationen werden in Dump- und Protokolldateien gespeichert.

Eine *Dump-Datei* enthält alle Informationen über den Arbeitsspeicher der Prozesse von Kaspersky Endpoint Security zum Zeitpunkt, als diese Dump-Datei erstellt wurde.

Eine *Protokolldatei* ermöglicht eine schrittweise Prüfung von ausgeführten Programmbefehlen. Dadurch lässt sich erkennen, auf welcher Etappe ein Fehler aufgetreten ist.

Dump-Dateien und Ablaufverfolgungsdateien können sensible Daten enthalten. Sie müssen selbst für den Schutz dieser Dateien sorgen, um die Sicherheit der Daten zu gewährleisten.

Dump-Dateien und Ablaufverfolgungsdateien bleiben während der gesamten Nutzungsdauer des Programms auf Ihrem Computer gespeichert und werden unwiderruflich gelöscht, wenn das Programm entfernt wird.

Sobald ein Sicherheitsprofil auf einen Computer angewendet wird, beginnt die Anwendung mit der Aufzeichnung von Dump-Dateien. Nach einer Fehlfunktion wird beim nächsten Anwendungsstart ein Fenster angezeigt, in dem Informationen für den Technischen Support geladen werden können. In diesem Fenster können Sie die Informationen über die erstellten Dump-Dateien prüfen und deren Übertragung an Kaspersky bestätigen.

Einstellungen für den Technischen Support

Einstellungen	Betriebssystem	Beschreibung
Dump-Erstellung AKTIVIERT	`Windows` `Linux`	Wenn die Dump-Aufzeichnung aktiviert ist, erstellt Kaspersky Endpoint Security bei einem Programmabsturz Dump-Dateien. `Linux` Dump-Dateien benötigen beträchtlichen freien Festplattenspeicher. Wenn weniger als 4 GB freier Speicherplatz auf der Festplatte vorhanden sind, kann die Dump-Aktivierung zu Platzproblemen führen.
Schutz für Dump- und Ablaufverfolgungsdateien AKTIVIERT	`Windows`	Wenn der Schutz für Dump-Dateien und Protokolldateien aktiviert ist, besitzen folgende Benutzer Zugriff auf die Dateien: • Zugriff auf Dump-Dateien besitzen der Systemadministrator, der lokale Administrator und der Benutzer, der die Aufzeichnung von Dump-Dateien und Protokolldateien aktiviert hat. • Zugriff auf Protokolldateien besitzen nur der Systemadministrator und der lokale Administrator.

Einstellungen	Betriebssystem	Beschreibung
Pfad für Code-Dumps	`Windows` `Linux`	Dump-Dateien werden in den folgenden Ordner gespeichert: • `Windows`: `%ProgramData%\Kaspersky Lab\KES.[AppVersion]\Traces` Sie können den Ordner für Dump-Dateien nicht ändern. • `Linux`: `var/opt/kaspersky/kesl/common/dumps` und `var/opt/kaspersky/kesl/common/dumps-user` 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 Verzeichnis mit den Dump-Dateien sind Root-Berechtigungen erforderlich.
Pfad für Ablaufverfolgungsdateien	`Windows` `Linux`	Ablaufverfolgungsdateien werden in den folgenden Ordnern gespeichert: • `Windows`: `%ProgramData%\Kaspersky Lab\KES.[AppVersion]\Traces` Sie können den Ordner für Ablaufverfolgungsdateien nicht ändern. • `Linux`: `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 Verzeichnis mit den Ablaufverfolgungsdateien sind Root-Berechtigungen erforderlich.
Maximale Größe einer Protokolldatei (MB)	`Linux`	In diesem Feld können Sie die maximale Größe einer Ablaufverfolgungsdatei für das Programm eingeben (in Megabyte).
Maximale Anzahl der Protokolldateien	`Linux`	In diesem Feld können Sie die maximale Anzahl von Ablaufverfolgungsdateien für das Programm eingeben.
Benutzerdefinierte Webressourcen des Technischen Supports	`Windows`	Tabelle mit Kontaktinformationen für Benutzer, die sich an den Technischen Support wenden möchten, falls in Kaspersky Endpoint Security Fehlfunktionen auftreten sollten. Sie können auch Vorlagen für Nachrichten konfigurieren, die den Benutzern erklären, wie sie technische Unterstützung erhalten können. Standardmäßig zeigt das Programm Links zur Kaspersky-Website an.

Berichte und Speicher

Für Windows, macOS und Linux

In diesem Abschnitt können Sie festlegen, wie Berichte über Ereignisse in Kaspersky Endpoint Security erstellt und aufbewahrt werden sollen, und Sie können die Speicherung von Objekten im Backup und in der Quarantäne konfigurieren.

Berichte

In *Berichten* werden protokolliert: Informationen über Ausführung der einzelnen Komponenten von Kaspersky Endpoint Security, über Ereignisse bei der Datenverschlüsselung, über die Ausführung der einzelnen Untersuchungsaufgaben, der Update-Aufgabe und der Aufgabe zur Integritätsprüfung, sowie über die allgemeine Programmausführung.

`Windows` Berichte werden im Ordner `C:\ProgramData\Kaspersky Lab\KES.12.4.0\Report` gespeichert.

Datenverwaltung

Das *Backup* ist ein Speicher für Backup-Kopien von Dateien, die bei der Desinfektion verändert oder gelöscht wurden. Eine *Backup-Kopie* ist die Kopie einer Datei, die vor der Desinfektion oder dem Löschen dieser Datei angelegt wird. Die Backup-Kopien von Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

Backup-Kopien von Dateien werden im folgenden Ordner gespeichert:

- `Windows`: `C:\ProgramData\Kaspersky Lab\KES.12.4.0\QB`
- `Linux`: `/var/opt/kaspersky/kesl/common/objects-backup/`

Vollständige Zugriffsrechte auf diesen Ordner besitzen die Benutzer der Gruppe „Administratoren“. Beschränkte Zugriffsrechte für diesen Ordner besitzt der Benutzer, unter dessen Benutzerkonto die Installation von Kaspersky Endpoint Security ausgeführt wurde.

Quarantäne

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.

Einstellungen für Berichte und Speicher

Einstellungen	Betriebssystem	Beschreibung
Berichte löschen nach (Tagen)	`Windows` `macOS`	Ist das Kontrollkästchen aktiviert, so ist die maximale Speicherdauer für Berichte durch das festgelegte Zeitintervall beschränkt. Nach Ablauf dieses Zeitraums löscht Kaspersky Endpoint Security automatisch die ältesten Einträge aus der Berichtsdatei.
Maximale Größe der Berichtsdatei (MB)	`Windows`	Ist das Kontrollkästchen aktiviert, so ist die maximale Größe der Berichtsdatei durch den festgelegten Wert beschränkt. Nach Erreichen der maximalen Berichtsdateigröße löscht Kaspersky Endpoint Security automatisch die ältesten Einträge aus der Berichtsdatei. Dadurch ist gewährleistet, dass die maximale Berichtsdateigröße nicht überschritten wird.
Nur aktuelle Ereignisse beibehalten	`macOS`	Wenn dieses Kontrollkästchen aktiviert ist, verfährt Kaspersky Endpoint Security beim Start einer Aufgaben wie folgt: Informationen über nicht-kritische Ereignisse, die seit dem letzten Aufgabenstart aufgetreten sind, werden gelöscht. Wichtige Notizen (z. B. Informationen über gefundene schädliche Objekte) werden im Bericht beibehalten.
Nicht-kritische Ereignisse protokollieren	`macOS`	Wenn dieses Kontrollkästchen aktiviert ist, protokolliert Kaspersky Endpoint Security nicht-kritische Ereignisse (z. B. informative Ereignisse) im Bericht. Nicht-kritische Ereignisse haben keinen Einfluss auf den Schutz.
Objekte löschen nach (Tagen)	`Windows` `macOS` `Linux`	Ist das Kontrollkästchen aktiviert, so ist die maximale Speicherdauer für Dateien durch das festgelegte Zeitintervall beschränkt. Nach Ablauf der maximalen Speicherdauer löscht Kaspersky Endpoint Security die ältesten Dateien aus dem Backup.
Maximale Größe des Backup-Speichers (MB)	`Windows` `Linux`	Ist das Kontrollkästchen aktiviert, so ist die maximale Backup-Größe durch den festgelegten Wert beschränkt. 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.
Maximale Größe der Quarantäne	`Windows` `Linux`	**Maximale Quarantäne-Größe (MB)**. Wenn das Kontrollkästchen aktiviert ist, ist die Quarantäne-Größe auf den festgelegten Wert beschränkt. Wenn die maximale Quarantäne-Größe erreicht wird, sendet Kaspersky Endpoint Security das Ereignis *Zu wenig Platz im Quarantäne-Speicher* an Kaspersky Security Center und erstellt ein Ereignis im Ereignisprotokoll des Betriebssystems. Die Anwendung stellt vorläufig keine neuen Objekte mehr unter Quarantäne. Sie müssen die Quarantäne manuell leeren. **Melden, wenn Quarantäne-Speicher diesen Wert erreicht (%)**. Schwellenwert für die Quarantäne. Sie können beispielsweise 50% als Quarantäne-Schwellenwert festlegen. Wenn die Quarantäne den Schwellenwert erreicht, sendet das Programm das entsprechende Ereignis an Kaspersky Security Center und protokolliert das Ereignis. Die Anwendung stellt weiterhin neue Objekte unter Quarantäne.

Integration mit KSC

Dieser Abschnitt beschreibt, wie Sie die Integration von Kaspersky Endpoint Security in Kaspersky Security Center konfigurieren können.

Einstellungen für die Integration in Kaspersky Security Center

Einstellungen	Betriebssystem	Beschreibung
Kaspersky Security Center als Proxyserver für die Aktivierung verwenden	`Windows` `macOS` `Linux`	Wenn dieses Kontrollkästchen aktiviert ist, verwendet die App den Kaspersky Security Center-Administrationsserver als Proxyserver für die Verbindung mit den Aktivierungsservern. Dies ist erforderlich, wenn die Anwendung in einem isolierten Netzwerksegment ohne Internetzugang anhand eines Aktivierungscodes aktiviert wird. Wenn Sie die App mit einer Schlüsseldatei aktivieren, ist kein Internetzugang erforderlich. Nicht anwendbar, wenn die App im Light Agent-Modus verwendet wird.
Datenübertragung an den Administrationsserver	`Windows` `macOS` `Linux`	Kategorien für Ereignisse auf den Client-Computern, über die Informationen an den Administrationsserver übertragen werden sollen. Sie können die Übertragung bestimmter Daten deaktivieren, um Speicherplatz auf dem Administrationsserver zu sparen. Das Programm sendet Ereignisse der folgenden Kategorien: • `Windows` **Über eine Bedrohungsentwicklungskette**. • `Windows` `macOS` `Linux` **Über Quarantäne-Dateien**. • `Windows` `Linux` **Über Backup-Dateien**. • `Windows` `Linux` **Über nicht verarbeitete Dateien**. • `Windows` `macOS` `Linux` **Über installierte Geräte**. • `Windows` `Linux` **Über gestartete Programme**. • `Windows` **Über Fehler bei der Dateiverschlüsselung**. • `Windows` **Statusbericht für Regeln der „Adaptiven Kontrolle von Anomalien“**. • `Windows` **Bericht über ausgelöste Regeln der „Adaptiven Kontrolle von Anomalien“**.

Konfiguration der Kommunikation mit dem Betriebssystem

Für Linux

Um ordnungsgemäß zu funktionieren, muss die Anwendung Systemereignisse im Sinne von Dateivorgängen und gestarteten Prozessen abfangen. Wenn das Abfangen von Systemereignissen von der Anwendung nicht verwendet wird, findet keine Dateiuntersuchung in Echtzeit statt. Dies reduziert die Schutzstufe des Geräts.

Konfiguration der Kommunikation mit dem Betriebssystem

Einstellungen	Betriebssystem	Beschreibung
Abfangmechanismus	`Linux`	Der von der Anwendung verwendete Mechanismus zum Abfangen von Systemereignissen: • **fanotify-Technologie**. 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 startet	`Linux`	Aktion, die das Programm ausführt, wenn das aktualisierbare Kernel-Modul nicht gestartet werden kann: • **fanotify-Technologie verwenden**. Wenn diese Option ausgewählt ist, wechselt das Programm zur Fanotify-Technologie zum Abfangen von Systemereignissen. • **Abfangen von Systemereignissen deaktivieren (verringert das Schutzniveau)**. Wenn das Abfangen von Systemereignissen von der Anwendung nicht verwendet wird, findet keine Dateiuntersuchung in Echtzeit statt. Dies reduziert die Schutzstufe des Geräts. Diese Einstellung ist verfügbar, wenn das Abfangverfahren **Aktualisierbares Kernel-Modul** ausgewählt ist.
Telemetrie-Quelle	`Linux`	Die Quelle, die Kaspersky Endpoint Security für die Telemetrie-Erfassung verwendet: • **Nur eBPF verwenden**. Es wird nur die eBPF-Technologie verwendet. • **Standard**. Es werden sowohl die eBPF-Technologie als auch der „auditd“-Dienst verwendet.

Einstellungen	Betriebssystem	Beschreibung
Funktionsmodus für auditd	`Linux`	In diesem Modus zeichnet der „auditd"-Dienst Audit-Ereignisse auf, um sie anschließend an Detection and Response-Lösungen zu übertragen: • **Ausschließlich**. Wenn diese Option ausgewählt ist, verwendet Kaspersky Endpoint Security nur den „auditd"-Dienst. Drittanbieter-Programme können keine Verbindung mit dem Audit-Datenstrom herstellen. • **Nicht ausschließlich**. Wenn diese Option ausgewählt ist, kann der „auditd"-Dienst mehrere Verbindungen von verschiedenen Prozessen, die das Systemaudit verwenden, akzeptieren.

Ereigniseinstellungen

Für Windows, macOS und Linux

In diesem Abschnitt können Sie Benachrichtigungen konfigurieren, die sich auf Ereignisse auf verwalteten Geräten und auf allgemeine Ereignisse beziehen. Die Benachrichtigungen können an die E-Mail-Adressen der Benutzer dieses Arbeitsbereichs gesendet werden.

Während der Ausführung der Anwendung treten verschiedene *Ereignisse* auf. Diese können rein informativ sein oder wichtige Informationen enthalten. Beispielsweise kann das Programm ein Ereignis verwenden, um über ein erfolgreiches Datenbanken-Update zu informieren oder auf einen kritischen Fehler in einer Komponente hinzuweisen.

Ereignisse in Kaspersky Endpoint Security können folgende Signifikanz haben:

- *Kritische Ereignisse* stellen eine ernsthafte Bedrohung für die Sicherheit des Computers dar (Erkennung von schädlichen Objekten, Schwachstellen, Probleme in Kaspersky Endpoint Security). Kritische Ereignisse erfordern Ihre sofortige Aufmerksamkeit. Es wird empfohlen, Benachrichtigungen für kritische Ereignisse aktiviert zu lassen.

- *Funktionsstörungen* sind Ereignisse, die bei Fehlfunktionen von Kaspersky Endpoint Security auftreten (Verarbeitungsfehler, fehlerhafte Aufgabeneinstellungen). Solche Ereignisse stellen keine direkte Bedrohung für die Sicherheit des Computers dar, erfordern jedoch Ihr Eingreifen, um die ordnungsgemäße Funktion von Kaspersky Endpoint Security und den Schutz Ihrer Geräte zu gewährleisten.

- *Warnungen* erfordern kein sofortiges Eingreifen, können aber auf eine zukünftige Bedrohung für die Sicherheit des Computers hinweisen.

- *Informative Meldungen*.

Unabhängig davon, ob Benachrichtigungen aktiviert oder deaktiviert sind, zeichnet Kaspersky Endpoint Security Informationen über alle Programmereignisse in den Programmberichten auf.

Sie können für jedes Ereignis in Kaspersky Endpoint Security eine passende Benachrichtigungsmethode festlegen:

- `Windows` **Per E-Mail informieren**.

- `Windows` **Im lokalen Bericht speichern**.

- `Windows` `macOS` **Auf dem Bildschirm anzeigen**.

- `Windows` `Linux` **Im System-Ereignisprotokoll speichern**.

Telemetrie-Einstellungen

Für Windows, macOS und Linux

In diesem Abschnitt können Sie das Senden von Telemetrie von verwalteten Geräten an Telemetrie-Erfassungsserver konfigurieren. *Telemetrie* ist eine Liste von Ereignissen, die auf dem geschützten Computer aufgetreten sind. Kaspersky Endpoint Security analysiert Telemetrie und sendet sie während der Synchronisierung an Kaspersky Anti Targeted Attack Platform oder an die 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.

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.

Im Abschnitt „Integrierte Agenten“ können Sie die Synchronisierungseinstellungen für die einzelnen integrierten Agenten verwalten und optimale Werte für die Netzwerkauslastung auswählen.

In diesem Abschnitt können Sie die folgenden Einstellungen konfigurieren:

- Ein- und Ausschlussregeln für Telemetrie.
- Erfassung von Telemetrie, die an KATA-Server, Telemetrie-Erfassungsserver oder Reaktionsserver gesendet wird.

Telemetrie für EDR Expert (on-premise)

Für Windows, macOS und Linux

Telemetrie-Einstellungen für EDR Expert (on-premise)

Einstellungen	Betriebssystem	Description
Telemetrie für EDR Expert (on-premise)	`Windows` `macOS` `Linux`	**Import** und **Export**. Sie können die Telemetrie-Einstellungen für EDR Expert (on-premise) 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 für die Einstellungen gesendeter Ereignisse anzulegen oder die Liste in eine andere Richtlinie zu migrieren.
Allgemeine Ausnahmen	`Windows` `macOS` `Linux`	Um die übertragenen Daten zu optimieren, können Sie Ausschlussregeln für bestimmte Ereignistypen konfigurieren. Telemetrie, die unter eine solche Regel fällt, wird von Kaspersky Endpoint Security nicht erfasst. Auf diese Weise können Sie den Datenverkehr reduzieren und die Verarbeitung von Ereignissen für vertrauenswürdige Objekten und Prozesse vermeiden. **Regelname**. **Aktion**: • **Nicht sammeln**. Wenn Sie diese Option auswählen, wird Telemetrie, die den Bedingungen der Regel entspricht, nicht von Kaspersky Endpoint Security erfasst. • **IOA ausschließen**. Wenn Sie diese Option auswählen, wird Telemetrie auf Basis einer IOA-Auslösungsregel, nicht von Kaspersky Endpoint Security erfasst. Ein *Angriffsindikator (IOA)* ist eine Regel, die ein verdächtiges Verhalten im System beschreibt. Solches Verhaltens kann auf einen gezielten Angriff hinweisen. **Bedingung**. Auslösebedingung für eine Regel. Geben Sie einen Telemetrie-Parameter, einen Bedingungsoperator und den Wert des Parameters an. Kaspersky Endpoint Security kombiniert Kriterien für die Regelauslösung standardmäßig mit einem logischen UND. Sie können mehrere Bedingungen oder Bedingungsgruppen mithilfe der logischen Operatoren UND und ODER hinzufügen.

Einstellungen	Betriebssystem	Description
Alle Ereignistypen	`Windows` `macOS` `Linux`	Liste der Ereignistypen, für welche die Telemetrie-Erfassung standardmäßig durch Kaspersky definiert wird. Sie können die Telemetrie für jeden Ereignistyp manuell aktivieren oder deaktivieren, sowie Aus- und Einschlussregeln für die Telemetrie konfigurieren.

Telemetrie für EDR (KATA)/NDR (KATA)

Für Windows und Linux

Um die Leistung zu verbessern und die Datenübertragung an den Telemetrie-Erfassungsserver zu optimieren, können Sie Telemetrie-Ausnahmen konfigurieren. Sie können beispielsweise festlegen, dass für einzelne Anwendungen keine Netzwerkkommunikationsdaten gesendet werden.

Einstellungen der Telemetrie-Ausnahmen für EDR (KATA)/NDR (KATA)

Einstellungen	Betriebssystem	Description
Ausgeschlossene Prozesse	`Windows` `Linux`	Daten, die sich auf Prozesse aus der Liste beziehen, werden von Kaspersky Endpoint Security nicht verarbeitet. **Telemetriegröße zum Senden optimieren**. Kaspersky Endpoint Security ermöglicht es, die Menge der übertragenen Daten zu optimieren und Ereignisse mit bestimmten Codes aus der Telemetrie auszuschließen: Code 102 (einfache Kommunikation) und 8 (Netzwerkaktivität des Prozesses) für das Microsoft SMB-Protokoll, den WinRM-Dienst und den Prozess klnagent.exe des Administrationsagenten sowie erweiterte Informationen über die Typen von Netzwerkpaketen für alle Typen von Netzwerkprotokollen. Kaspersky Endpoint Security kombiniert Kriterien für die Regelauslösung mit einem logischen UND. **Prozess** und **Übergeordneter Prozess**: • **Vollständiger Pfad**. Vollständiger Pfad der Datei, einschließlich Name und Erweiterung. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske. • **Befehlszeilentext**. Befehl zum Ausführen der Datei. • **Beschreibung**. Wert des Parameters FileDescription aus einer RT_VERSION-Ressource (VersionInfo). • **Ursprünglicher Dateiname**. Wert des Parameters OriginalFilename aus einer RT_VERSION-Ressource (VersionInfo). • **Version**. Wert des Parameters FileVersion aus einer RT_VERSION-Ressource (VersionInfo). • **Dateiprüfsummen**. MD5 und SHA256. Sie können die Datei auch manuell auswählen. Dann werden die Felder für die ausgewählte Datei automatisch von der App ausgefüllt. In 64-Bit-Betriebssystemen müssen Sie die Parameter der 64-Bit-Version der ausführbaren Datei eines Prozesses aus dem Ordner `C:\windows\system32` manuell eingeben, da das Programm die Parameterfelder der ausführbaren Datei mit Daten aus den Eigenschaften der 32-Bit-Version derselben ausführbaren Datei im Ordner `C:\windows\syswow64` ausfüllt. Wenn Sie beispielsweise `C:\windows\system32\cmd.exe` auswählen, zeigt das Plug-in die Parameter von `C:\windows\syswow64\cmd.exe` an. Dieses Verhalten geht auf Besonderheiten des Betriebssystems zurück. **Für die folgenden Ereignistypen verwenden**: • **Dateiänderung**. • **Netzwerk-Ereignisse**. • **Prozess: interaktive Konsoleneingabe**. • **Modul geladen**. • **Registrierung geändert**. • **DNS-Protokolle**. • **Prozesszugriff**. • **Code-Injektion**. • `Windows` **WMI-Abfrage**. • **Pipe**. • **LDAP**. • `Windows` **AMSI**.

Einstellungen	Betriebssystem	Description
Ausgeschlossene Netzwerkkommunikationen	`Windows` `Linux`	Daten, die sich auf Netzwerkkommunikationen aus der Liste beziehen, werden von Kaspersky Endpoint Security nicht verarbeitet. In der Ausschlussregel können Sie folgende Werte angeben: **Regelname**. **Richtung**. **Protokoll**. **Raw-Socket**. **Protokollnummer**. **Lokale Adresse**. Die Netzwerkadresse des Computers, für den Kaspersky Endpoint Security Telemetriedaten aus dem Netzwerkverkehr ausschließt. **Lokaler Port oder Bereich**. **Remote-Adresse**. Die Netzwerkadresse des Computers, für den Kaspersky Endpoint Security Telemetriedaten aus dem Netzwerkverkehr ausschließt. **Remote-Port oder -Bereich**. Für IP-Adressen wird nur das IPv4-Format unterstützt. **Regel auf die ausgewählten Programme anwenden**. Wenn dieses Kontrollkästchen aktiviert ist, schließt Kaspersky Endpoint Security für die ausführbaren Dateien der Programme aus dieser Liste die EDR-Telemetrie aus dem Netzwerkverkehr aus.
Ausgeschlossene Vorgänge mit Dateien	`Windows` `Linux`	Dateivorgänge aus der Liste werden von Kaspersky Endpoint Security nicht verarbeitet. In der Ausschlussregel können Sie folgende Werte angeben: **Regelname**. **Dateiname oder Maske**. Der Dateiname oder die Maske, auf den bzw. die Kaspersky Endpoint Security die Ausschlussregel anwendet, wenn auf die Datei zugegriffen wird. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske. **Dateivorgang auswählen**. Typ des Dateivorgangs, für den die Regel gelten soll. **Vorheriger Pfad**. Kaspersky Endpoint Security kombiniert Kriterien für die Regelauslösung mit einem logischen UND. **Prozess** und **Übergeordneter Prozess**: • **Vollständiger Pfad**. Vollständiger Pfad der Datei, einschließlich Name und Erweiterung. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske. • **Befehlszeilentext**. Befehl zum Ausführen der Datei. • **Beschreibung**. Wert des Parameters FileDescription aus einer RT_VERSION-Ressource (VersionInfo). • **Ursprünglicher Dateiname**. Wert des Parameters OriginalFilename aus einer RT_VERSION-Ressource (VersionInfo). • **Version**. Wert des Parameters FileVersion aus einer RT_VERSION-Ressource (VersionInfo). • **Dateiprüfsummen**. MD5 und SHA256. Sie können die Datei auch manuell auswählen. Dann werden die Felder für die ausgewählte Datei automatisch von der App ausgefüllt. In 64-Bit-Betriebssystemen müssen Sie die Parameter der 64-Bit-Version der ausführbaren Datei eines Prozesses aus dem Ordner `C:\windows\system32` manuell eingeben, da das Programm die Parameterfelder der ausführbaren Datei mit Daten aus den Eigenschaften der 32-Bit-Version derselben ausführbaren Datei im Ordner `C:\windows\syswow64` ausfüllt. Wenn Sie beispielsweise `C:\windows\system32\cmd.exe` auswählen, zeigt das Plug-in die Parameter von `C:\windows\syswow64\cmd.exe` an. Dieses Verhalten geht auf Besonderheiten des Betriebssystems zurück.

Einstellungen	Betriebssystem	Description
Ausgeschlossene DNS-Vorgänge	`Windows` `Linux`	Die DNS-Vorgänge aus der Liste werden von Kaspersky Endpoint Security nicht verarbeitet. In der Ausschlussregel können Sie folgende Werte angeben: **Regelname**. Kaspersky Endpoint Security kombiniert Kriterien für die Regelauslösung mit einem logischen UND. **Prozess** und **Übergeordneter Prozess**: • **Vollständiger Pfad**. Vollständiger Pfad der Datei, einschließlich Name und Erweiterung. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske. • **Befehlszeilentext**. Befehl zum Ausführen der Datei. • **Beschreibung**. Wert des Parameters FileDescription aus einer RT_VERSION-Ressource (VersionInfo). • **Ursprünglicher Dateiname**. Wert des Parameters OriginalFilename aus einer RT_VERSION-Ressource (VersionInfo). • **Version**. Wert des Parameters FileVersion aus einer RT_VERSION-Ressource (VersionInfo). • **Dateiprüfsummen**. MD5 und SHA256. Sie können die Datei auch manuell auswählen. Dann werden die Felder für die ausgewählte Datei automatisch von der App ausgefüllt. In 64-Bit-Betriebssystemen müssen Sie die Parameter der 64-Bit-Version der ausführbaren Datei eines Prozesses aus dem Ordner `C:\windows\system32` manuell eingeben, da das Programm die Parameterfelder der ausführbaren Datei mit Daten aus den Eigenschaften der 32-Bit-Version derselben ausführbaren Datei im Ordner `C:\windows\syswow64` ausfüllt. Wenn Sie beispielsweise `C:\windows\system32\cmd.exe` auswählen, zeigt das Plug-in die Parameter von `C:\windows\syswow64\cmd.exe` an. Dieses Verhalten geht auf Besonderheiten des Betriebssystems zurück. **DNS-Vorgang**: • **IP-Adresse des DNS-Servers**. • **Abfrageoptionen**. • **Status**. • **Domänenname**. • **ID des Einstellungstyps**. • **Antwortdaten**. Inhalt der DNS-Antwort auf die Abfrage.

Einstellungen	Betriebssystem	Description
Ausgeschlossene LDAP-Vorgänge	`Windows`	Die LDAP-Vorgänge aus der Liste werden von Kaspersky Endpoint Security nicht verarbeitet. In der Ausschlussregel können Sie folgende Werte angeben: **Regelname**. Kaspersky Endpoint Security kombiniert Kriterien für die Regelauslösung mit einem logischen UND. **Prozess** und **Übergeordneter Prozess**: • **Vollständiger Pfad**. Vollständiger Pfad der Datei, einschließlich Name und Erweiterung. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske. • **Befehlszeilentext**. Befehl zum Ausführen der Datei. • **Beschreibung**. Wert des Parameters FileDescription aus einer RT_VERSION-Ressource (VersionInfo). • **Ursprünglicher Dateiname**. Wert des Parameters OriginalFilename aus einer RT_VERSION-Ressource (VersionInfo). • **Version**. Wert des Parameters FileVersion aus einer RT_VERSION-Ressource (VersionInfo). • **Dateiprüfsummen**. MD5 und SHA256. Sie können die Datei auch manuell auswählen. Dann werden die Felder für die ausgewählte Datei automatisch von der App ausgefüllt. In 64-Bit-Betriebssystemen müssen Sie die Parameter der 64-Bit-Version der ausführbaren Datei eines Prozesses aus dem Ordner `C:\windows\system32` manuell eingeben, da das Programm die Parameterfelder der ausführbaren Datei mit Daten aus den Eigenschaften der 32-Bit-Version derselben ausführbaren Datei im Ordner `C:\windows\syswow64` ausfüllt. Wenn Sie beispielsweise `C:\windows\system32\cmd.exe` auswählen, zeigt das Plug-in die Parameter von `C:\windows\syswow64\cmd.exe` an. Dieses Verhalten geht auf Besonderheiten des Betriebssystems zurück. **LDAP-Vorgang**: • **LDAP-Suchbereich**. LDAP-Suchbereich. Einer der folgenden Werte ist möglich: ADS_SCOPE_BASE, ADS_SCOPE_ONELEVEL, ADS_SCOPE_SUBTREE. • **Filter**. • **Definierter Name für Suche nach LDAP-Objekten**. Name des Eintrags im LDAP-Verzeichnis. • **Objekt-Attribute, die zur Suche nach LDAP-Vorgängen dienen**. Attribute, die in der Abfrage als Rückgabewerte festgelegt sind.

Einstellungen	Betriebssystem	Description
Ausgeschlossene Prozesszugriffsabfragen	`Windows`	Anfragen für den Zugriff auf Prozesse aus dieser Liste werden von Kaspersky Endpoint Security nicht verarbeitet. In der Ausschlussregel können Sie folgende Werte angeben: **Regelname**. Kaspersky Endpoint Security kombiniert Kriterien für die Regelauslösung mit einem logischen UND. **Prozess**, **Übergeordneter Prozess**, **Datei des Zielprozesses**, **Handle an den Quellprozess** und **Handle an den Zielprozess**. • **Vollständiger Pfad**. Vollständiger Pfad der Datei, einschließlich Name und Erweiterung. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske. • **Befehlszeilentext**. Befehl zum Ausführen der Datei. • **Ursprünglicher Dateiname**. Wert des Parameters OriginalFilename aus einer RT_VERSION-Ressource (VersionInfo). • **Version**. Wert des Parameters FileVersion aus einer RT_VERSION-Ressource (VersionInfo). • **Dateiprüfsummen**. MD5 und SHA256. Sie können die Datei auch manuell auswählen. Dann werden die Felder für die ausgewählte Datei automatisch von der App ausgefüllt. In 64-Bit-Betriebssystemen müssen Sie die Parameter der 64-Bit-Version der ausführbaren Datei eines Prozesses aus dem Ordner `C:\windows\system32` manuell eingeben, da das Programm die Parameterfelder der ausführbaren Datei mit Daten aus den Eigenschaften der 32-Bit-Version derselben ausführbaren Datei im Ordner `C:\windows\syswow64` ausfüllt. Wenn Sie beispielsweise `C:\windows\system32\cmd.exe` auswählen, zeigt das Plug-in die Parameter von `C:\windows\syswow64\cmd.exe` an. Dieses Verhalten geht auf Besonderheiten des Betriebssystems zurück. **Prozesszugriffsabfragen**: • **Vorgangstyp**. • **Zugriff auf den Prozess angefordert**. • **Aufruflistenüberwachung**.

Einstellungen	Betriebssystem	Description
Ausgeschlossene Code-Injektionen	`Windows`	Code-Injektionen für Prozesse aus der Liste werden von Kaspersky Endpoint Security nicht verarbeitet. In der Ausschlussregel können Sie folgende Werte angeben: **Regelname**. Kaspersky Endpoint Security kombiniert Kriterien für die Regelauslösung mit einem logischen UND. **Prozess** und **Übergeordneter Prozess**: • **Vollständiger Pfad**. Vollständiger Pfad der Datei, einschließlich Name und Erweiterung. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske. • **Befehlszeilentext**. Befehl zum Ausführen der Datei. • **Beschreibung**. Wert des Parameters FileDescription aus einer RT_VERSION-Ressource (VersionInfo). • **Ursprünglicher Dateiname**. Wert des Parameters OriginalFilename aus einer RT_VERSION-Ressource (VersionInfo). • **Version**. Wert des Parameters FileVersion aus einer RT_VERSION-Ressource (VersionInfo). • **Dateiprüfsummen**. MD5 und SHA256. Sie können die Datei auch manuell auswählen. Dann werden die Felder für die ausgewählte Datei automatisch von der App ausgefüllt. In 64-Bit-Betriebssystemen müssen Sie die Parameter der 64-Bit-Version der ausführbaren Datei eines Prozesses aus dem Ordner `C:\windows\system32` manuell eingeben, da das Programm die Parameterfelder der ausführbaren Datei mit Daten aus den Eigenschaften der 32-Bit-Version derselben ausführbaren Datei im Ordner `C:\windows\syswow64` ausfüllt. Wenn Sie beispielsweise `C:\windows\system32\cmd.exe` auswählen, zeigt das Plug-in die Parameter von `C:\windows\syswow64\cmd.exe` an. Dieses Verhalten geht auf Besonderheiten des Betriebssystems zurück. **Code-Injektionen**: • **Zugriffsmethode**. • **Aufrufliste**. Die API-Aufrufliste zum Zeitpunkt, als die Funktion, die sich auf die Code-Injektion bezieht, abgefangen wurde • **Modifizierte Befehlszeile**. • **Injektionsadresse**. Adresse im Adressraum des Zielprozesses, in dem der remote ausgeführte Code abgelegt wurde. Dieses Feld bleibt leer, wenn die Code-Injektion mithilfe der Methoden SET_WINDOWS_HOOK und ARG_SPOOFING erreicht wurde. • **Modifizierte Befehlszeile**. • **Eingefügter DLL-Name**. Name der DLL, die die Abfangroutine enthält, und Name der Funktion, an die die Kontrolle nach der Injektion übergeben wird. Dieses Feld wird ausgefüllt, wenn die Code-Injektion mithilfe der Methode SET_WINDOWS_HOOK erreicht wurde. • **Eingefügter DLL-Pfad**. Pfad der DLL, die die Abfangroutine enthält. Dieses Feld wird ausgefüllt, wenn die Code-Injektion mithilfe der Methode SET_WINDOWS_HOOK erreicht wurde.

Einstellungen	Betriebssystem	Description
Ausgeschlossene WMI-Abfragen	`Windows`	WMI-Anfragen aus der Liste werden von Kaspersky Endpoint Security nicht verarbeitet. In der Ausschlussregel können Sie folgende Werte angeben: **Regelname**. Kaspersky Endpoint Security kombiniert Kriterien für die Regelauslösung mit einem logischen UND. **Prozess** und **Übergeordneter Prozess**: • **Vollständiger Pfad**. Vollständiger Pfad der Datei, einschließlich Name und Erweiterung. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske. • **Befehlszeilentext**. Befehl zum Ausführen der Datei. • **Beschreibung**. Wert des Parameters FileDescription aus einer RT_VERSION-Ressource (VersionInfo). • **Ursprünglicher Dateiname**. Wert des Parameters OriginalFilename aus einer RT_VERSION-Ressource (VersionInfo). • **Version**. Wert des Parameters FileVersion aus einer RT_VERSION-Ressource (VersionInfo). • **Dateiprüfsummen**. MD5 und SHA256. Sie können die Datei auch manuell auswählen. Dann werden die Felder für die ausgewählte Datei automatisch von der App ausgefüllt. In 64-Bit-Betriebssystemen müssen Sie die Parameter der 64-Bit-Version der ausführbaren Datei eines Prozesses aus dem Ordner `C:\windows\system32` manuell eingeben, da das Programm die Parameterfelder der ausführbaren Datei mit Daten aus den Eigenschaften der 32-Bit-Version derselben ausführbaren Datei im Ordner `C:\windows\syswow64` ausfüllt. Wenn Sie beispielsweise `C:\windows\system32\cmd.exe` auswählen, zeigt das Plug-in die Parameter von `C:\windows\syswow64\cmd.exe` an. Dieses Verhalten geht auf Besonderheiten des Betriebssystems zurück. **WMI-Abfragen**: • **WMI-Vorgangstyp**. • **Remote-Abfrage**. • **Name eines Computers, der einen WMI-Befehl ausgeführt hat**. • **WMI-Benutzerkonto**. • **Ausgeführter WMI-Befehl**. • **WMI-Namensraum**. • **Filter für WMI-Ereignis-Consumer**. • **Name des erstellten WMI-Ereignis-Consumers**. • **Quellcode eines WMI-Ereignis-Consumers**.

Einstellungen	Betriebssystem	Description
Ausgeschlossene Pipe-Vorgänge	`Windows`	Pipe-Vorgänge aus der Liste werden von Kaspersky Endpoint Security nicht verarbeitet. In der Ausschlussregel können Sie folgende Werte angeben: **Regelname**. Kaspersky Endpoint Security kombiniert Kriterien für die Regelauslösung mit einem logischen UND. **Prozess** und **Übergeordneter Prozess**: • **Vollständiger Pfad**. Vollständiger Pfad der Datei, einschließlich Name und Erweiterung. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske. • **Befehlszeilentext**. Befehl zum Ausführen der Datei. • **Beschreibung**. Wert des Parameters FileDescription aus einer RT_VERSION-Ressource (VersionInfo). • **Ursprünglicher Dateiname**. Wert des Parameters OriginalFilename aus einer RT_VERSION-Ressource (VersionInfo). • **Version**. Wert des Parameters FileVersion aus einer RT_VERSION-Ressource (VersionInfo). • **Dateiprüfsummen**. MD5 und SHA256. Sie können die Datei auch manuell auswählen. Dann werden die Felder für die ausgewählte Datei automatisch von der App ausgefüllt. In 64-Bit-Betriebssystemen müssen Sie die Parameter der 64-Bit-Version der ausführbaren Datei eines Prozesses aus dem Ordner `C:\windows\system32` manuell eingeben, da das Programm die Parameterfelder der ausführbaren Datei mit Daten aus den Eigenschaften der 32-Bit-Version derselben ausführbaren Datei im Ordner `C:\windows\syswow64` ausfüllt. Wenn Sie beispielsweise `C:\windows\system32\cmd.exe` auswählen, zeigt das Plug-in die Parameter von `C:\windows\syswow64\cmd.exe` an. Dieses Verhalten geht auf Besonderheiten des Betriebssystems zurück. **Pipe-Vorgänge**: • **Pipe-Name**. • **Vorgangstyp**.

Einstellungen	Betriebssystem	Description
Ausgeschlossene Registrierungsänderungen	`Windows`	Registrierungsänderungen aus der Liste werden von Kaspersky Endpoint Security nicht verarbeitet. In der Ausschlussregel können Sie folgende Werte angeben: **Regelname**. Kaspersky Endpoint Security kombiniert Kriterien für die Regelauslösung mit einem logischen UND. **Prozess** und **Übergeordneter Prozess**: • **Vollständiger Pfad**. Vollständiger Pfad der Datei, einschließlich Name und Erweiterung. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske. • **Befehlszeilentext**. Befehl zum Ausführen der Datei. • **Beschreibung**. Wert des Parameters FileDescription aus einer RT_VERSION-Ressource (VersionInfo). • **Ursprünglicher Dateiname**. Wert des Parameters OriginalFilename aus einer RT_VERSION-Ressource (VersionInfo). • **Version**. Wert des Parameters FileVersion aus einer RT_VERSION-Ressource (VersionInfo). • **Dateiprüfsummen**. MD5 und SHA256. Sie können die Datei auch manuell auswählen. Dann werden die Felder für die ausgewählte Datei automatisch von der App ausgefüllt. In 64-Bit-Betriebssystemen müssen Sie die Parameter der 64-Bit-Version der ausführbaren Datei eines Prozesses aus dem Ordner `C:\windows\system32` manuell eingeben, da das Programm die Parameterfelder der ausführbaren Datei mit Daten aus den Eigenschaften der 32-Bit-Version derselben ausführbaren Datei im Ordner `C:\windows\syswow64` ausfüllt. Wenn Sie beispielsweise `C:\windows\system32\cmd.exe` auswählen, zeigt das Plug-in die Parameter von `C:\windows\syswow64\cmd.exe` an. Dieses Verhalten geht auf Besonderheiten des Betriebssystems zurück. **Registrierungsänderungen**: • **Vorgangstyp**. • **Pfad**. Pfad des Registrierungsschlüssels, in dem die Änderung vorgenommen wurde. • **Name des Wertes**. Name des geänderten Werts (z. B. RegistrySizeLimit). • **Wert**. • **Vollständiger Name der Registrierungsdatei**.
Ausgeschlossene Vorgänge mit Geräten	`Windows`	Vorgänge, die sich auf USB-Geräte aus der Liste beziehen, werden von Kaspersky Endpoint Security nicht verarbeitet. In der Ausschlussregel können Sie folgende Werte angeben: **Regelname**. **Gerätetyp**. **Geräte-ID**. **Gerätename**.

KUMA-Telemetrie

Für Windows

Das Senden von Ereignissen an den KUMA-Server ist standardmäßig deaktiviert. Um sicherzustellen, dass KUMA ordnungsgemäß funktioniert, müssen Sie das Senden von Telemetrie aktivieren. Sie können eine Ereignisquelle aus den Standardprotokollen auswählen: *Application*, *Security* oder *System*. Sie können auch das Protokoll eines Drittanbieterprogramms angeben. Um die Leistung zu verbessern und die Datenübertragung an den KUMA-Server zu optimieren, können Sie bestimmte Ereignisprotokolle manuell hinzufügen.

Einstellungen für KUMA-Telemetrie

Einstellungen	Betriebssystem	Description
Windows-Ereignisprotokolle	`Windows`	Windows-Protokollereignisse, die die Anwendung an KUMA sendet. Sie können Protokolle manuell hinzufügen oder eine json-Datei mit Einstellungen importieren. Sie können für jedes Ereignisprotokoll auswählen, auf welche Weise es gesendet werden soll: • **Alle Ereignisse senden**. In diesem Modus sendet das Programm alle Ereignisse aus dem Windows-Protokoll, unter Ausnahme von Ereignissen, die den Ausschlussregeln hinzugefügt wurden. • **Nur ausgewählte Ereignisse senden**. In diesem Modus sendet das Programm nur Ereignisse, die in Einschlussregeln hinzugefügt wurden. Sie können auch Ausschluss- oder Einschlussregeln für den entsprechenden Modus der Ereignisübertragung konfigurieren. Um Regeln hinzuzufügen, müssen Sie die Ereignis-ID aus dem Windows-Ereignisprotokoll angeben. Sie können mehrere Ereignis-IDs in einer Regel angeben. Wenn Sie mehrere Ereignis-IDs angeben, verwenden Sie Kommas als Trennzeichen.

Integrierte Agenten

Managed Detection and Response

Für Windows, macOS und Linux

Kaspersky Endpoint Security unterstützt die Integration in die Managed Detection and Response-Lösung. 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“.

Sie müssen die folgenden Komponenten aktivieren, damit „Managed Detection and Response“ funktioniert:

- Kaspersky Security Network (erweiterter Modus)
- Verhaltensanalyse

Das Aktivieren dieser Komponenten ist obligatorisch. Andernfalls funktioniert „Kaspersky Managed Detection and Response“ nicht, da die erforderlichen Telemetriedaten nicht empfangen werden.

Einstellungen der Komponente „Managed Detection and Response“

Einstellungen	Betriebssystem	Beschreibung

MDR-Konfigurationsdatei	`Windows`
	`macOS`
	`Linux`
		Die BLOB-Datei enthält die Client-ID und Informationen zur Lizenz für Kaspersky Managed Detection and Response. Die BLOB-Datei befindet sich im ZIP-Archiv der MDR-Konfigurationsdatei. Sie können das ZIP-Archiv in der Konsole von Kaspersky Managed Detection and Response abrufen. Ausführliche Informationen zur BLOB-Datei finden Sie in der Hilfe zu „Kaspersky Managed Detection and Response“.

Endpoint Detection and Response Optimum

Für Windows, macOS und Linux

Kaspersky Endpoint Security enthält einen integrierten Agenten für die Lösung Kaspersky Endpoint Detection and Response Optimum (im Folgenden auch „EDR Optimum“). *Kaspersky Endpoint Detection and Response* umfasst eine Reihe von Lösungen, mit denen die IT-Infrastruktur eines Unternehmens vor komplexen Cyberbedrohungen geschützt wird. Diese Lösungen kombinieren die automatische Erkennung von Bedrohungen mit der Fähigkeit, auf diese Bedrohungen zu reagieren. Dadurch lassen sich komplexe Angriffe wie neue Exploits, Ransomware, dateilose Angriffe und Methoden mit legitimen Systemtools abwehren.

Kaspersky Endpoint Detection and Response analysiert potenziell gefährliche Aktivitäten auf den Benutzergeräten und versorgt die *Sicherheitsbeauftragten* oder den *Administrator* mit Informationen über einen möglichen Angriff. Dadurch können zeitnahe Reaktionen ergriffen werden, oder es werden automatisch konfigurierte Reaktionen ausgelöst.

Damit Endpoint Detection and Response funktioniert, müssen Sie die folgenden Komponenten aktivieren:

- Komponente "Schutz vor bedrohlichen Dateien".
- Schutz vor Web-Bedrohungen
- Schutz vor E-Mail-Bedrohungen
- Exploit-Prävention
- Verhaltensanalyse
- Programm-Überwachung
- Rollback von schädlichen Aktionen
- Adaptive Kontrolle von Anomalien

Die Liste der Komponenten kann je nach Plattform unterschiedlich sein.

Einstellungen der Komponente „Endpoint Detection and Response“

Einstellungen	Betriebssystem	Beschreibung
Erweiterte Protokollierung der Systemaktivität aktivieren	`Windows` `macOS` `Linux`	Diese Einstellung trägt zur ordnungsgemäßen Ausführung der Aufgabe **Retrospektive IOC-Untersuchung** bei. Diese Option ist mit einer starken Nutzung von Computerressourcen verbunden.
Netzwerkisolation	`Windows` `macOS` `Linux`	Automatische Isolation des Computers vom Netzwerk als Reaktion auf erkannte Bedrohungen. Wenn die Netzwerkisolation aktiviert ist, trennt die Anwendung alle aktiven Verbindungen und blockiert alle neuen TCP/IP-Verbindungen auf dem Computer. Die Anwendung lässt nur die folgenden Verbindungen zu: • Verbindungen, die als Ausnahmen von der Netzwerkisolation festgelegt sind. • Verbindungen, die durch die Dienste von Kaspersky Endpoint Security initiiert werden • Verbindungen, die durch den Kaspersky Security Center Administrationsagent initiiert werden
Isolation eines Geräts automatisch beenden nach (Std.)	`Windows` `macOS` `Linux`	Die Netzwerkisolation kann automatisch nach einem bestimmten Zeitraum deaktiviert werden oder manuell.

Einstellungen	Betriebssystem	Beschreibung
Ausnahmen für die Netzwerkisolation	`Windows` `macOS` `Linux`	Liste mit Regeln für Ausnahmen von der Netzwerkisolation. Netzwerkverbindungen, die diesen Regeln entsprechen, werden auf Computern nicht gesperrt, wenn die Netzwerkisolation aktiviert ist. Zur Konfigurierung von Ausnahmen für die Netzwerkisolation können Sie eine Liste von *Standardnetzwerkprofilen* verwenden. Zu den Ausnahmen gehören standardmäßig Netzwerkprofile mit Regeln, die sicherstellen, dass Geräte mit den Rollen DNS/DHCP-Server und DNS/DHCP-Client unterbrechungsfrei funktionieren. Außerdem können Sie die Einstellungen von Standardnetzwerkprofilen ändern oder Ausnahmen manuell definieren. In den Richtlinieneigenschaften angegebene Ausnahmen werden nur angewendet, wenn die Netzwerkisolation als Reaktion auf eine erkannte Bedrohung automatisch aktiviert wird. In den Computereigenschaften angegebene Ausnahmen werden nur angewendet, wenn die Netzwerkisolation manuell in den Computereigenschaften in der Kaspersky Security Center-Konsole oder in den Alarm-Details aktiviert wurde.
Ausführungsprävention	`Windows` `macOS` `Linux`	Steuert die Ausführung von ausführbaren Dateien und Skripten sowie das Öffnen von Dateien im Office-Format. Sie können beispielsweise die Ausführung von Anwendungen verhindern, die auf dem ausgewählten Computer als unsicher gelten. Die Ausführungsprävention unterstützt eine Reihe von Office-Dateierweiterungen und Skriptinterpretern. Um die Komponente Ausführungsprävention zu verwenden, müssen Sie die Regeln für die Ausführungsprävention hinzufügen.
Aktion beim Ausführen oder Öffnen eines verbotenen Objekts	`Windows` `macOS` `Linux`	**Blockieren und dem Ereignisprotokoll hinzufügen**. In diesem Modus sperrt die Anwendung die Ausführung von Objekten oder das Öffnen von Dokumenten, die den Kriterien der Präventionsregel entsprechen. Außerdem veröffentlicht das Programm im Systemereignisprotokoll und in Kaspersky Security Center ein Ereignis über Versuche, Objekte auszuführen oder Dokumente zu öffnen. **Dem Ereignisprotokoll hinzufügen**. In diesem Modus veröffentlicht Kaspersky Endpoint Security im Systemereignisprotokoll und in Kaspersky Security Center ein Ereignis über Versuche, ausführbare Objekte auszuführen oder Dokumente zu öffnen, die den Kriterien der Präventionsregel entsprechen. Der Versuch, das Objekt auszuführen oder das Dokument zu öffnen, wird jedoch nicht blockiert. Dieser Modus ist standardmäßig ausgewählt.
Regeln zur Ausführungsprävention	`Windows` `macOS` `Linux`	Eine *Regel für die Ausführungsprävention* ist eine Reihe von Kriterien, nach denen die Anwendung auf die Ausführung eines Objekts reagiert, beispielsweise wenn die Objektausführung blockiert wird. Die Anwendung identifiziert Dateien anhand von Pfaden oder Prüfsummen, die auf MD5- und SHA256-Hash-Algorithmen beruhen.
Groß-/Kleinschreibung beim Pfad berücksichtigen	`Linux`	Wenn dieses Kontrollkästchen aktiviert ist, berücksichtigt das Programm die Groß-/Kleinschreibung beim Erstellen von Regeln zur Ausführungsprävention.
Cloud Sandbox	`Windows` `macOS` `Linux`	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. Eine KSN-Verbindung ist erforderlich, um Informationen über die zu analysierenden Objekte abzurufen.

Endpoint Detection and Response Expert (on-premise)

Für Windows, macOS und Linux

Endpoint Detection and Response Expert Version 7.1 oder älter

Kaspersky Endpoint Security unterstützt die Komponente „Kaspersky Endpoint Detection and Response Expert“ (Version 7.1 und älter, im Folgenden auch als „EDR (KATA)“ bezeichnet) als Teil der Lösung „Kaspersky Anti Targeted Attack Platform“. Die Lösung *Kaspersky Anti Targeted Attack Platform* dient der rechtzeitigen Erkennung komplexer Bedrohungen. Dazu zählen beispielsweise gezielte Angriffe, hoch entwickelte hartnäckige Bedrohungen (APT, Advanced Persistent Threat) und Zero-Day-Angriffe. Kaspersky Anti Targeted Attack Platform umfasst drei Funktionseinheiten:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Sie können alle Funktionseinheiten oder einzelne Funktionseinheiten separat erwerben. Einzelheiten über diese Lösung finden Sie in der Hilfe zu „Kaspersky Anti Targeted Attack 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 (Telemetriedaten) werden an den Kaspersky Anti Targeted Attack Platform-Server gesendet. In diesem Fall sendet Kaspersky Endpoint Security an den Kaspersky Anti Targeted Attack Platform-Server auch Informationen über die von der App erkannten Bedrohungen sowie Informationen über die Verarbeitungsergebnisse dieser Bedrohungen.

Die Integration von EDR (KATA) und NDR (KATA) wird in der Kaspersky Security Center-Konsole konfiguriert. Anschließend wird der integrierte Agent über die Kaspersky Anti Targeted Attack Platform-Konsole verwaltet, was sich beispielsweise auch auf folgende Vorgänge bezieht: Aufgaben ausführen, Objekten in der Quarantäne verwalten und Berichte anzeigen.

Endpoint Detection and Response Expert Version 8.0 oder höher

Kaspersky Endpoint Security unterstützt Kaspersky-Lösungen der Klasse „Endpoint Detection and Response Expert“ (Version 8.0 und höher, im Folgenden auch als „EDR Expert (on-premise)“ bezeichnet). Zu diesen Lösungen gehört beispielsweise Kaspersky Symphony XDR. *Endpoint Detection and Response Expert (on-premise)* ist eine Cybersicherheitslösung für Unternehmen. Diese Lösung kann ein Unternehmen vor den meisten Arten von Cyberrisiken schützen und deckt die wichtigsten Verbreitungsszenarien für Bedrohungen ab.

EDR Expert (on-premise) analysiert Protokolle und Telemetriedaten, die von der Unternehmensinfrastruktur empfangen werden, um automatisch Angriffe zu erkennen, und ermöglicht die Untersuchung von Vorfällen. Dazu dient ein einheitlicher Untersuchungsgraph, der alle in EDR Expert (on-premise) erfassten Ereignisse kombiniert, einschließlich der Ereignisse aus Kaspersky-Programmen und Informationssicherheitsprodukten von Drittanbietern.

Komponenten, die für Endpoint Detection and Response Expert erforderlich sind

Damit Endpoint Detection and Response Expert funktioniert, müssen Sie die folgenden Komponenten aktivieren:

- Schutz vor bedrohlichen Dateien
- Schutz vor Web-Bedrohungen
- Schutz vor E-Mail-Bedrohungen
- Exploit-Prävention
- Verhaltensanalyse
- Programm-Überwachung
- AMSI-Schutz
- Untersuchung im Hintergrund
- Kaspersky Security Network

Die Liste der Komponenten kann je nach Plattform unterschiedlich sein.

Einstellungen der Komponenten von Endpoint Detection and Response Expert (on-premise)

Einstellungen	Betriebssystem	Description
Lösung „Endpoint Detection and Response Expert“	`Windows` `macOS` `Linux`	Endpoint Detection and Response Expert-Lösungen, in die Kaspersky Endpoint Security integriert werden kann. • **Endpoint Detection and Response Expert (Version 7.1 oder älter)**. • **Endpoint Detection and Response Expert (ab Version 8.0)**.
Verbindungseinstellungen	`Windows` `macOS` `Linux`	Verwalten Sie die folgenden Einstellungen für Verbindungen mit KATA- oder Telemetrie-Erfassungsservern: • **Server-Verbindungstimeout**. 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.

Einstellungen	Betriebssystem	Description
Synchronisierungsanfrage an Server senden alle (Min.) *(nur für Endpoint Detection and Response Expert Version 7.1 oder älter verfügbar)*	`Windows` `macOS` `Linux`	Häufigkeit der an den Server gesendeten Synchronisierungsanfragen. Während der Synchronisierung sendet Kaspersky Endpoint Security Informationen über geänderte Einstellungen und Aufgaben der App.
Verbindung mit KATA-Servern / Verbindung mit Telemetrie-Erfassungsservern	`Windows` `macOS` `Linux`	Geben Sie die IP-Adresse (IPv4 oder IPv6) und den Port für die Verbindung mit dem Kaspersky Anti Targeted Attack Platform-Server oder dem Telemetrie-Erfassungsserver ein. Sie können mehrere Adressen für den Central Node-Server (KATA) oder für den Telemetrie-Erfassungsserver 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. Die Lösungen EDR (KATA) und EDR Expert (on-premise) unterscheiden sich in der Architektur. Für die Telemetrieverarbeitung verwendet EDR Expert (on-premise) einen Telemetrie-Erfassungsserver, während EDR (KATA) einen Central Node-Server verwendet. Wenn Sie das Programm in EDR Expert (on-premise) integrieren, müssen Sie daher einen Telemetrie-Erfassungsserver hinzufügen.
Telemetriedaten an KATA senden / Telemetrie an Telemetrie-Erfassungsserver senden	`Windows` `macOS` `Linux`	Je nach ausgewählter Lösung kann mit dieser Funktion das Senden von Telemetrie an den KATA-Server oder Telemetrie-Erfassungsserver vollständig verhindert werden. Wenn Sie beispielsweise Kaspersky Anti Targeted Attack Platform zusammen mit einer anderen Lösung verwenden, die ebenfalls Telemetrie verwendet, können Sie das Senden von Telemetrie für KATA (EDR) deaktivieren. Dadurch lässt sich die Serverlast für diese Lösungen optimieren. Wenn Sie die Managed Detection and Response-Lösung und KATA (EDR) bereitgestellt haben, können Sie MDR-Telemetrie verwenden und Threat Response-Aufgaben in KATA (EDR) erstellen.
Telemetrie nur mit IOA senden *(nur für Endpoint Detection and Response Expert Version 8.0 oder höher verfügbar)*	`Windows` `Linux`	Dies ermöglicht, die Telemetrie zu optimieren und nur Telemetrie mit IOA zu 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.
Maximale Verzögerung der Ereignisübertragung (Sek.)	`Windows` `macOS` `Linux`	Die App synchronisiert sich mit dem Server, um Ereignisse nach Ablauf des Synchronisierungsintervalls zu senden.
Maximale Anzahl der Ereignispakete	`Windows`	Das Programm synchronisiert sich mit dem Server, wenn sich genügend Ereignisse im Puffer befinden.
Anforderungsbegrenzung aktivieren	`Windows` `macOS` `Linux`	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. **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. 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.
Verbindung mit Reaktionsservern *(nur für Endpoint Detection and Response Expert Version 8.0 oder höher verfügbar)*	`Windows` `macOS` `Linux`	Einstellungen der Verbindung mit Reaktionsservern. Geben Sie die IP-Adresse des Reaktionsservers (IPv4, IPv6) und den Port für die Serververbindung ein. Sie können mehrere Adressen für Reaktionsserver 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.

Einstellungen	Betriebssystem	Description

Verbindungseinstellungen
(nur für Endpoint Detection and Response Expert Version 8.0 oder höher verfügbar)
	`Windows`
	`macOS`
	`Linux`
		Konfigurieren Sie die folgenden Einstellungen für die Verbindung zum Reaktionsserver:
		• **Server-Verbindungstimeout**. Maximales Timeout für die Antwort des Reaktionsservers. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Reaktionsserver zu verbinden.
		• **Serverzertifikat**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Reaktionsserver.
		• **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Herstellen einer sicheren Verbindung zwischen Kaspersky Endpoint Security und dem Reaktionsserver. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Reaktionsservers aktivieren, dann einen Krypto-Container anfordern und ein Kennwort für den Krypto-Container festlegen. 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 Einstellungen des Reaktionsservers 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.

Network Detection and Response (KATA)

Für Windows und Linux

Kaspersky Endpoint Security unterstützt die Arbeit mit der Komponente „Kaspersky Network Detection and Response“ als Teil der Lösung „Kaspersky Anti Targeted Attack Platform“ (EDR (KATA)). Die Lösung *Kaspersky Anti Targeted Attack Platform* dient der rechtzeitigen Erkennung komplexer Bedrohungen. Dazu zählen beispielsweise gezielte Angriffe, hoch entwickelte hartnäckige Bedrohungen (APT, Advanced Persistent Threat) und Zero-Day-Angriffe. Kaspersky Anti Targeted Attack Platform umfasst drei Funktionseinheiten:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Sie können alle Funktionseinheiten oder einzelne Funktionseinheiten separat erwerben. Einzelheiten über diese Lösung finden Sie in der Hilfe zu „Kaspersky Anti Targeted Attack 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 (Telemetriedaten) werden an den Kaspersky Anti Targeted Attack Platform-Server gesendet. In diesem Fall sendet Kaspersky Endpoint Security an den Kaspersky Anti Targeted Attack Platform-Server auch Informationen über die von der App erkannten Bedrohungen sowie Informationen über die Verarbeitungsergebnisse dieser Bedrohungen.

Die Integration von EDR (KATA) und NDR (KATA) wird in der Kaspersky Security Center-Konsole konfiguriert. Anschließend wird der integrierte Agent über die Kaspersky Anti Targeted Attack Platform-Konsole verwaltet, was sich beispielsweise auch auf folgende Vorgänge bezieht: Aufgaben ausführen, Objekten in der Quarantäne verwalten und Berichte anzeigen.

Damit Network Detection and Response (KATA) funktioniert, müssen die folgenden Komponenten aktiviert sein:

- Komponente "Schutz vor bedrohlichen Dateien".
- Schutz vor Web-Bedrohungen
- Schutz vor E-Mail-Bedrohungen
- Exploit-Prävention
- Verhaltensanalyse
- Programm-Überwachung
- AMSI-Schutz
- Untersuchung im Hintergrund
- Kaspersky Security Network

Die Liste der Komponenten kann je nach Plattform unterschiedlich sein.

Einstellungen der Komponente „Network Detection and Response" (KATA)

Einstellungen	Betriebssystem	Beschreibung
Verbindungseinstellungen für KATA-Server	`Windows` `Linux`	**Server-Verbindungstimeout**. 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.
Verbindung mit KATA-Servern	`Windows` `Linux`	Einstellungen für die Verbindung mit Kaspersky Anti Targeted Attack Platform-Servern. Geben Sie die IP-Adresse (IPv4 oder IPv6) und den Port des Central Node-Servers für die Verbindung ein. 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.
Synchronisierungsanfrage an KATA-Server senden alle (Min.)	`Windows` `Linux`	Häufigkeit der an den Server gesendeten Synchronisierungsanfragen. Während der Synchronisierung sendet Kaspersky Endpoint Security Informationen über geänderte Einstellungen und Aufgaben der App.
Maximale Verzögerung der Ereignisübertragung (Sek.)	`Windows` `Linux`	Die App synchronisiert sich mit dem Server, um Ereignisse nach Ablauf des Synchronisierungsintervalls zu senden.

Einstellungen	Betriebssystem	Beschreibung
Anforderungsbegrenzung aktivieren	`Windows` `Linux`	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. **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. 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.

Sandbox

Für Windows und Linux

Kaspersky Endpoint Security unterstützt die Integration in die Lösung „Kaspersky Sandbox“ und in die Sandbox-Komponente, die Teil der Lösung „Kaspersky Anti Targeted Attack Platform“ ist. Die Komponente *„Sandbox“* erkennt und blockiert automatisch komplexe Bedrohungen auf Computern. „Sandbox“ analysiert das Verhalten von Objekten, um schädliche Aktivitäten zu erkennen sowie Aktivitäten, die für gezielte Angriffe auf die IT-Infrastruktur eines Unternehmens charakteristisch sind. „Sandbox“ analysiert und untersucht Objekte auf speziellen Servern, auf denen virtuelle Abbilder von Microsoft Windows-Betriebssystemen bereitstehen („Sandbox“-Server). Einzelheiten über diese Lösung finden Sie in der Hilfe zu Kaspersky Sandbox und in der Hilfe zu Kaspersky Anti Targeted Attack Platform.

Die Komponente „KATA Sandbox“ erlaubt es, Dateien sowohl automatisch zu untersuchen als auch manuell aus dem Kontextmenü einer Datei.

KATA Sandbox erfordert die Bereitstellung von Kaspersky Anti Targeted Attack Platform 7.0 höher.

Einstellungen der Komponente „Sandbox“

Einstellungen	Betriebssystem	Beschreibung
Integrationsmodus	`Windows` `Linux`	**Kaspersky Sandbox**. Integration in die Lösung Kaspersky Sandbox. Dateien, die in Kaspersky Sandbox untersucht werden sollen, werden vom Programm nur im automatischen Modus gesendet. **KATA Sandbox**. Integration in die Sandbox-Komponente der Lösung Kaspersky Anti Targeted Attack Platform. Sie können auswählen, in welchem Modus die Dateien zur Untersuchung übertragen werden: • **Manuell**. Der Benutzer übermittelt die zu untersuchende Datei manuell über das Kontextmenü (**An Sandbox senden**). • **Automatisch**. Das Programm erkennt Objekte automatisch und sendet sie zur Untersuchung an die Sandbox. • **Kombiniert**. Das Programm sendet Objekte automatisch zur Untersuchung an Sandbox. Bei Bedarf kann der Benutzer auch einzelne Dateien über das Kontextmenü zur Untersuchung senden.
Verbindung mit Sandbox-Servern	`Windows` `Linux`	**Kaspersky Sandbox**. Verbindungseinstellungen für die „Sandbox“-Server. Die Server verwenden bereitgestellte virtuelle Abbilder von Microsoft Windows-Betriebssystemen, um die zu untersuchenden Objekte auszuführen. Geben Sie die IP-Adresse des Sandbox-Servers (IPv4, IPv6 oder DNS) und den Port für die Serververbindung ein. **KATA Sandbox**. Einstellungen der Verbindung zum Central Node-Server. Central Node wählt die optimalen Untersuchungseinstellungen und verteilt die Last zwischen den Sandbox-Servern. Geben Sie die IP-Adresse des Central Node-Servers (IPv4, IPv6 oder DNS) und den Port für die Serververbindung ein.

Einstellungen	Betriebssystem	Beschreibung
Einstellungen der Serververbindung	`Windows` `Linux`	**Server-Verbindungstimeout**. Timeout für Verbindungen zum Sandbox-Server (für Kaspersky Sandbox) oder Central Node-Server (für KATA). Nach Ablauf des festgelegten Timeouts sendet Kaspersky Endpoint Security eine Anfrage an den nächsten Server. Bei niedriger Verbindungsgeschwindigkeit oder instabiler Verbindung können Sie das Verbindungstimeout für den Server erhöhen. Das empfohlene Anforderungstimeout ist 0,5 Sekunden oder weniger. **Anforderungswarteschlange**. Größe des Ordners der Anforderungswarteschlange. Wenn mehrere Objekte zur Untersuchung in der Sandbox gesendet werden, erstellt Kaspersky Endpoint Security eine Warteschlange für Anfragen. Die Größe des Ordners der Anforderungswarteschlange ist standardmäßig auf 100 MB begrenzt. Wenn die maximale Größe erreicht wird, fügt „Sandbox" keine neuen Anforderungen zur Warteschlange hinzu und sendet ein entsprechendes Ereignis an Kaspersky Security Center. Abhängig von Ihrer Serverkonfiguration können Sie die Größe des Ordners der Anforderungswarteschlange anpassen. **TLS-Serverzertifikat**. Um eine vertrauenswürdige Verbindung mit dem Sandbox-Server (für Kaspersky Sandbox) oder dem Central Node-Server (für KATA) zu konfigurieren, müssen Sie ein TLS-Zertifikat erstellen. Anschließend müssen Sie das Zertifikat mithilfe einer Richtlinie dem Computer hinzufügen. Außerdem müssen Sie das Zertifikat dem Sandbox-Server (für Kaspersky Sandbox) oder dem Central Node-Server (für KATA) hinzufügen. **Zwei-Wege-Authentifizierung verwenden** (nur für KATA Sandbox). 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.
Aktion beim Fund einer Bedrohung	`Windows` `Linux`	**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.
IOC-Untersuchungsbereich	`Windows` `Linux`	**Bereiche mit kritischen Dateien**. Wenn diese Option ausgewählt ist, untersucht Kaspersky Endpoint Security nur die wichtigen Dateibereichen des Computers auf IOCs, z. B. ausgewählte Verzeichnisse mit Benutzerprofilen und kritischen Systemobjekten. **Dateibereiche auf Systemlaufwerken des Computers**. Wenn diese Option ausgewählt ist, untersucht Kaspersky Endpoint Security das Systemlaufwerk des Computers auf IOCs. Unabhängig vom ausgewählten Untersuchungsbereich, wird auch unter dem Dateipfad, in dem die Bedrohung erkannt wurde, nach IOCs gesucht.
IOC-Untersuchungsaufgabe ausführen	`Windows` `Linux`	**Manuell**. In diesem Ausführungsmodus können Sie die Aufgabe *IOC-Untersuchung* zu einem geeigneten Zeitpunkt manuell starten. **Automatisch**. In diesem Modus führt Kaspersky Endpoint Security die *IOC-Untersuchung* automatisch aus, wenn eine Bedrohung erkannt wird. `Windows` **Nur ausführen, wenn der Computer inaktiv ist**. In diesem Modus führt Kaspersky Endpoint Security die Aufgabe *IOC-Untersuchung* aus, wenn der Bildschirmschoner aktiv oder der Bildschirm gesperrt ist. Wenn der Benutzer den Computer entsperrt, hält Kaspersky Endpoint Security die Aufgabe an. Es kann also mehrere Tage dauern, bis die Aufgabe abgeschlossen wird.

Integration mit KUMA

Für Windows und Linux

Kaspersky Endpoint Security 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.

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.

Das Senden von Ereignissen an den KUMA-Server ist standardmäßig deaktiviert. Um die ordnungsgemäße Funktion von KUMA zu gewährleisten, aktivieren Sie zuerst das Senden von Telemetriedaten an KUMA im Abschnitt Allgemeine Einstellungen → Telemetrie-Einstellungen.

Kaspersky Endpoint Security stellt nicht alle Funktionen eines Agenten für KUMA bereit. Die App sendet nur Ereignisse ohne Markierungen an KUMA. Um auf alle KUMA-Funktionen zugreifen zu können, müssen Sie eine Lizenz erwerben und die Lösung gemäß dem KUMA-Administratorhandbuch bereitstellen.

Einstellungen der KUMA-Komponente

Einstellungen	Betriebssystem	Beschreibung
Einstellungen der Serververbindung	`Windows` `Linux`	**Server-Verbindungstimeout**. Maximales Timeout für die Antwort des KUMA-Servers. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen KUMA-Server zu verbinden. **Serverzertifikat**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem KUMA-Server. Ein TLS-Zertifikat können Sie in der Konsole von Kaspersky Unified Monitoring and Analysis Platform anfordern (siehe Anleitung für Kaspersky Unified Monitoring and Analysis Platform). **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Aufbau einer sicheren Verbindung zwischen Kaspersky Endpoint Security und KUMA. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie in der KUMA-Konsole in den TCP-Konnektor-Einstellungen den TLS-Modus **Custom PFX** auswählen (siehe Einstellungen für den TCP-Konnektor in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform). Dann müssen Sie 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. Nachdem Sie die KUMA-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.
Maximale Verzögerung beim Versenden von Ereignissen (Sek.)	`Windows` `Linux`	Die App synchronisiert sich mit dem Server, um Ereignisse nach Ablauf des Synchronisierungsintervalls zu senden.
TLS-Verschlüsselung verwenden	`Windows` `Linux`	Wenn diese Funktion aktiviert ist, verwendet Kaspersky Endpoint Security ein TLS-Zertifikat, um eine vertrauenswürdige Verbindung mit dem KUMA-Server herzustellen.
Verbindung mit KUMA-Servern	`Windows` `Linux`	Einstellungen für die Verbindung mit dem KUMA-Server. Geben Sie eine IP-Adresse (IPv4 oder IPv6), ein Verbindungsprotokoll und einen Port für die Verbindung zum Server an. Sie können mehrere Adressen für KUMA-Server hinzufügen. 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.

Light Agent-Modus

Einstellungen der SVM-Erkennung

Für Windows und Linux

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 Dateifragmente, die untersucht werden müssen, an die SVM. Die Untersuchungsergebnisse sind für alle virtuellen Maschinen verfügbar, auf denen Light Agent installiert ist (die SharedCache-Technologie). Somit erhöht die SharedCache-Technologie 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. Die Komponente Integrationsserver dient der Interaktion zwischen den einzelnen Komponenten der Lösung und der virtuellen Infrastruktur. 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.

Einstellungen der SVM-Erkennung

Einstellungen	Betriebssystem	Beschreibung
Integrationsserver verwenden	`Windows` `Linux`	Ein Integrationsserver ist in großen virtuellen Infrastrukturen nützlich, da der Integrationsserver die Last zwischen den SVMs automatisch verteilt. Geben Sie die Einstellungen für die Verbindung zum Integrationsserver ein: • IP-Adresse im IPv4-Format oder als vollqualifizierter Domänenname (FQDN) des Geräts mit installiertem Integrationsserver. • Portnummer für die Verbindung zum Integrationsserver. Der Standardport ist 7271. • Kennwort für das Administratorkonto des Integrationsservers (Kennwort des Benutzerkontos „admin").
Benutzerdefinierte Liste mit SVM-Adressen verwenden	`Windows` `Linux`	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. Sie können mehrere IP-Adressen oder vollständige Domänennamen der SVMs in einer neuen Zeile eingeben. 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.

Einstellung der Verbindung mit dem Integrationsserver

Für Windows und Linux

Der *Integrationsserver* ist eine Komponente der Lösung. Er ermöglicht die Interaktion von Kaspersky Security for Virtualization Light Agent mit der virtuellen Infrastruktur. Der Integrationsserver führt eine Liste der SVMs, mit denen eine Verbindung hergestellt werden kann. Light Agent stellt eine Verbindung mit dem Integrationsserver her und ruft die Liste mit SVM-Adressen ab.

Ein Integrationsserver ist in großen virtuellen Infrastrukturen nützlich, da der Integrationsserver die Last zwischen den SVMs automatisch verteilt. Der Integrationsserver ruft Informationen über verfügbare SVMs ab, analysiert diese Informationen und stellt den Light Agents eine Liste mit Schutzservern (SVM) zur Verfügung, die für eine Verbindung optimal sind.

Einstellungen	Betriebssystem	Beschreibung
Adresse	`Windows` `Linux`	IP-Adresse im IPv4-Format oder als vollqualifizierter Domänenname (FQDN) des Integrationsservers. Wenn als Adresse ein NetBIOS-Name, localhost oder 127.0.0.1 angegeben ist, wird die Verbindung zum Integrationsserver mit einem Fehler beendet.
Port	`Windows` `Linux`	Portnummer für die Verbindung zum Integrationsserver. Der Standardport ist 7271.
Authentifizierung am Integrationsserver	`Windows` `Linux`	Kennwort für das Administratorkonto des Integrationsservers (Kennwort des Benutzerkontos `admin`). Nachdem die Verbindung mit Integrationsserver mittels Administratorrechten hergestellt wurde, wird das Kennwort Benutzerkontos `agent` automatisch in die Richtlinie übertragen, die zur Verbindung von Light Agents mit dem Integrationsserver verwendet wird.

Tag für die Verbindung zur SVM

Für Windows und Linux

Mehrere Light Agents können sich mit einer SVM verbinden. Um Auslastung durch Light Agent-Verbindungen auszugleichen, können Sie im Abschnitt „Einstellungen zur SVM-Ermittlung“ 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 Lizenzschlüssel für EDR Optimum (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.

Aktivieren Sie das Kontrollkästchen **Tag für die Verbindung verwenden**, um Tags für die Verbindung von Light Agents zu verwenden. Geben Sie ein Tag für die Verbindung zur SVM ein. Als Tag können Sie eine Zeichenkette von höchstens 255 Zeichen Länge eingeben. Sie können jedes Zeichen mit Ausnahme von `;` verwenden.

Algorithmus der SVM-Auswahl

Für Windows und Linux

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.

Einstellungen für den Algorithmus der SVM-Auswahl

Einstellungen	Betriebssystem	Beschreibung
Standard-Algorithmus zur SVM-Auswahl verwenden	`Windows` `Linux`	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. Um eine SVM als lokal zu identifizieren, verwendet Light Agent zuerst den Standort der SVM in der virtuellen Infrastruktur. Wenn sich SVMs im selben Hypervisor wie der Light Agent befinden, betrachtet Light Agent diese SVMs als lokal. In einigen virtuellen Infrastrukturen müssen Sie lokale SVMs mithilfe einer Konfigurationsdatei manuell angeben. 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.
Erweiterten Algorithmus zur SVM-Auswahl verwenden	`Windows` `Linux`	Mit dem erweiterten Algorithmus können Sie Auswahlkriterien für lokale SVMs manuell angeben oder die lokale SVM-Ermittlung deaktivieren. Dazu müssen Sie den Standort der SVM in der virtuellen Infrastruktur auswählen: Hypervisor, Cluster oder Datencenter. Sie müssen also den Bereich auswählen, in dem die lokalen SVMs erkannt werden sollen. Wenn der Light Agent keine Verbindung zu einer lokalen SVM im konfigurierten Erkennungsbereich herstellen kann, wird der Verbindungsversuch abgebrochen. Der erweiterte Algorithmus ermöglicht es auch, die Erkennung lokaler SVMs für den Light Agent zu deaktivieren. In diesem Fall wählt Light Agent die SVMs aus, mit denen im Hinblick auf die gesamte virtuelle Infrastruktur am wenigsten Light Agents verbunden sind.

Schutz der Verbindung

Für Windows und Linux

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 Verbindungsschutz mithilfe der Verschlüsselung kann die Leistung von Kaspersky Security for Virtualization Light Agent beeinträchtigen.

Anhang 6. 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.

Netzwerkadresse und Protokoll des Dienstes	Description
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.

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 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	
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	–

Programmkomponente	Empfohlener Komponentenstatus	Empfehlungen
Inventar	Deaktiviert	–
Gerätekontrolle	Deaktiviert	–
Programmkontrolle	Deaktiviert	–
Firewall	Deaktiviert	–
Web-Kontrolle	Deaktiviert	–
Überwachung der Systemintegrität	Enabled	Untersuchungsbereiche hinzufügen: • /etc • /opt/kaspersky/kesl/ • /opt/kaspersky/ksc64
Prüfung der Systemintegrität	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	–
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 Benutzeroberfläche	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.

Network Detection and Response (KATA)

Wenn Sie Kaspersky Endpoint Security für Linux zusammen mit Network Detection and Response (KATA) verwenden, empfehlen wir, die in diesem Artikel beschriebenen Einstellungen zu verwenden.

Lesen Sie auch die Dokumentation der Lösung Kaspersky Anti Targeted Attack (KATA) Platform.

Einstellungen für Kaspersky Endpoint Security für Linux auf Servern mit der Sensor-Komponente

Empfohlene Einstellungen für Sensor-Server

Programmkomponente	Empfohlener Komponentenstatus	Empfehlungen
Schutz vor bedrohlichen Dateien	Enabled	Schutzausnahmen hinzufügen: • `[container-name:*kata_scanner*]/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/storage/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*preprocessor_icap*]/tmp/content` • `[container-name:*preprocessor_span*]/tmp/suricata` • `[container-name:*preprocessor_span*]/mnt/kaspersky/nta` • `[container-name:*preprocessor_smtp*]/tmp/` • `[container-name:*preprocessor_pop*]/tmp/` • `[container-name:*sandbox_scan*]/tmp/` • `[container-name:*]/var/log/kaspersky`
Schadsoftware-Untersuchung	Deaktiviert	–
Untersuchung von Wechseldatenträgern	Deaktiviert	–
Verhaltensanalyse	Enabled	Verwenden Sie die Standardeinstellungen.
Schutz vor Netzwerkbedrohungen	Deaktiviert	–
Schutz vor Web-Bedrohungen	Deaktiviert	–
Schutz vor Verschlüsselung	Deaktiviert	–
Container untersuchen	Enabled	Aktivieren Sie die Container-Überwachung, um laufende Container und Namensräume in Echtzeit zu untersuchen `NamespaceMonitoring=Yes`
Inventar	Deaktiviert	–
Gerätekontrolle	Deaktiviert	–
Programmkontrolle	Deaktiviert	–
Firewall	Deaktiviert	–
Web-Kontrolle	Deaktiviert	–
Überwachung der Systemintegrität	Deaktiviert	–
Prüfung der Systemintegrität	Deaktiviert	–

Programmkomponente	Empfohlener Komponentenstatus	Empfehlungen
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 Benutzeroberfläche	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	–
Protokolldateien	–	Ändern Sie das Verzeichnis für Protokolldateien in ein Verzeichnis außerhalb des Verzeichnisses `/var/log/kaspersky`. Verwenden Sie beispielsweise das Verzeichnis `/var/log/kesl`.
Globale Ausnahmen	Konfiguriert	Schließen Sie die folgenden Mount-Punkte aus: • `/apt_spool` • `/storage` • `/var/lib/postgresql` • `/var/lib/clickhouse` • `/tmp` • `/tmp/*` Die Ausnahme der Mount-Punkte /tmp und /tmp/* gilt für NDR (KATA)-Server der Version 10.0 und früher. • `/varog/kaspersky` • `/var/opt/kaspersky` • `/data` • `/data/volumes/dumps`

Einstellungen für Kaspersky Endpoint Security für Linux auf Servern mit der Central Node-Komponente

Empfohlene Einstellungen für Central Node-Server

Programmkomponente	Empfohlener Komponentenstatus	Empfehlungen
Schutz vor bedrohlichen Dateien	Enabled	Schutzausnahmen hinzufügen: • `[container-name:*edr_synchronizer*]/tmp/` • `[container-name:*ids_alert_syncer*]/tmp/` • `[container-name:kata_product_main_1_kata_scanner]/storage` • `[container-name:kata_product_main_1_postgresql_server]/var/lib/postgresql` • `[container-name:kata_product_main_1_clickhouse]/var/lib/clickhouse` • `[container-name:*kata_scanner*]/storage/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/var/opt/kaspersky/apt-agents` • `[container-name:*kata_scanner*]/var/lib/nginx/body` • `[container-name:*kata_scanner*]/apt_spool` • `[container-name:*kata_scanner*]/tmp/` • `[container-name:*kafka*]/tmp/` • `[container-name:*ksn_proxy*]/tmp/` • `[container-name:*preprocessor_smtp*]/tmp/` • `[container-name:*preprocessor_pop*]/tmp/` • `[container-name:*preprocessor_icap*]/tmp/` • `[container-name:*preprocessor_span*]/tmp/` • `[container-name:*sandbox_scan*]/tmp/` • `[container-name:*statistics_clickhouse_importer*]/tmp/` • `[container-name:*updates_consistency_checker*]/tmp/` • `[container-name:*web_backend*]/tmp/` • `[container-name:*]/var/opt/kaspersky` • `/tmp/` • `/var/log/kaspersky`
Schadsoftware-Untersuchung	Deaktiviert	–
Untersuchung von Wechseldatenträgern	Deaktiviert	–
Verhaltensanalyse	Enabled	Verwenden Sie die Standardeinstellungen.
Schutz vor Netzwerkbedrohungen	Deaktiviert	–
Schutz vor Web-Bedrohungen	Deaktiviert	–
Schutz vor Verschlüsselung	Deaktiviert	–
Container untersuchen	Enabled	Aktivieren Sie die Container-Überwachung, um laufende Container und Namensräume in Echtzeit zu untersuchen `NamespaceMonitoring=Yes`
Inventar	Deaktiviert	–
Gerätekontrolle	Deaktiviert	–
Programmkontrolle	Deaktiviert	–
Firewall	Deaktiviert	–
Web-Kontrolle	Deaktiviert	–
Überwachung der Systemintegrität	Deaktiviert	–
Prüfung der Systemintegrität	Deaktiviert	–
Endpoint Detection and Response Expert (On-Premises)	Deaktiviert	–

Programmkomponente	Empfohlener Komponentenstatus	Empfehlungen
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 Benutzeroberfläche	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	–
Protokolldateien	–	Ändern Sie das Verzeichnis für Protokolldateien in ein Verzeichnis außerhalb des Verzeichnisses `/var/log/kaspersky`. Verwenden Sie beispielsweise das Verzeichnis `/var/log/kesl`.
Globale Ausnahmen	Konfiguriert	Mount-Punkte zu Ausnahmen hinzufügen: • `/apt_spool` • `/storage` • `/var/lib/postgresql` • `/var/lib/clickhouse` • `/tmp` • `/tmp/*` Die Ausnahme der Mount-Punkte /tmp und /tmp/* gilt für NDR (KATA)-Server der Version 10.0 und früher. • `/var/log/kaspersky` • `/var/opt/kaspersky` • `/data`

Kaspersky Unified Monitoring and Analysis Platform

Wenn Sie Kaspersky Endpoint Security für Linux zusammen mit Kaspersky Unified Monitoring and Analysis Platform verwenden, wird empfohlen, die in diesem Artikel beschriebenen Einstellungen zu verwenden.

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`
Schutz vor Web-Bedrohungen	Deaktiviert	–
Schutz vor Verschlüsselung	Deaktiviert	–
Container untersuchen	Deaktiviert	–
Inventar	Deaktiviert	–
Gerätekontrolle	Deaktiviert	–
Programmkontrolle	Deaktiviert	–
Firewall	Deaktiviert	–
Web-Kontrolle	Deaktiviert	–
Überwachung der Systemintegrität	Deaktiviert	–
Prüfung der Systemintegrität	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 Benutzeroberfläche	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	–

Informationsquellen zu Kaspersky Endpoint Security

Seite für Kaspersky Endpoint Security in der Wissensdatenbank

Die Wissensdatenbank ist ein spezieller Bereich auf der Support-Webseite.

Auf der Seite von Kaspersky Endpoint Security in der Wissensdatenbank finden Sie nützliche Informationen, Tipps und Antworten auf häufig gestellte Fragen. Dabei werden Fragen wie Kauf, Installation und Verwendung der Anwendung behandelt.

Die Artikel der Wissensdatenbank behandeln neben Fragen zu Kaspersky Endpoint Security auch andere Anwendungs von Kaspersky. In der Wissensdatenbank finden Sie auch Neuigkeiten über den Technischen Support.

Diskussion über Kaspersky-Apps im Forum

Wenn Ihre Frage nicht dringend ist, können Sie mit Kaspersky-Experten und anderen Benutzern in unserem Forum darüber diskutieren.

Im Forum können Sie vorhandene Themen nachlesen, Kommentare schreiben und neue Themen zur Diskussion stellen.

Glossar

Abonnement

Verwendung der Anwendung mit den ausgewählten Einstellungen (Enddatum, Anzahl der Geräte). Sie können ein Abonnement anhalten, fortsetzen, automatisch verlängern lassen oder kündigen.

Administrationsgruppe

Gruppe von Geräten, die aufgrund ihrer ausgeführten Funktionen und der darauf installierten Gruppe von Kaspersky-Anwendungen in Kaspersky Security Center zusammengefasst wurden. Geräte werden zur bequemen Handhabung als Einheiten in Gruppen zusammengefasst. Eine Administrationsgruppe kann andere Gruppen beinhalten. Für alle in der Administrationsgruppe installierten Anwendungen können Gruppenrichtlinien angelegt und Gruppenaufgaben erstellt werden.

Administrationsserver

Eine Komponente von Kaspersky Security Center, die der zentralen Speicherung von Informationen über alle im Unternehmensnetzwerk installierten Kaspersky-Programme dient. Die Verwaltung dieser Programme erfolgt ebenfalls über diese Komponente.

Aktive Richtlinie

Die Richtlinie, die von der Anwendung derzeit zur Vermeidung von Datenverlust verwendet wird. Die Anwendung kann mehrere Richtlinien gleichzeitig verwenden.

Aktiver Schlüssel

Ein Schlüssel, der momentan der Anwendung verwendet wird.

Anwendungseinstellungen

Einstellungen für die Ausführung der Anwendung, die für alle Aufgabentypen gleich sind und den Gesamtbetrieb der Anwendung regeln, zum Beispiel Leistungseinstellungen der Anwendung, Berichtseinstellungen und Backup-Einstellungen.

App-Datenbanken

Datenbanken, die Informationen über Bedrohungen der Computersicherheit enthalten, die Kaspersky zum Veröffentlichungsdatum der Datenbank bekannt waren. Die Datenbanken der Anwendung werden von Kaspersky-Experten erstellt und stündlich aktualisiert.

Ausnahme

Ein *Ausschluss* ist ein Objekt, das von der Untersuchung durch eine Kaspersky-Anwendung ausgeschlossen ist. Es können Dateien eines bestimmten Formats, Dateien nach Maske, ein bestimmter Bereich (z. B. ein Ordner oder ein Programm), Programmprozesse oder Objekte nach Namen gemäß der Klassifizierung der Viren-Enzyklopädie von der Untersuchung ausgeschlossen werden. Für jede Aufgabe können separate Ausnahmen angegeben werden.

Autostart-Objekte

Bestimmte Anwendungen, die für den Start und den korrekten Betrieb des auf Ihrem Computer installierten Betriebssystems und der Software erforderlich sind. Bei jedem Start des Betriebssystem werden diese Objekte gestartet. Es gibt Viren, die in der Lage sind, eben solche Objekte zu infizieren, was beispielsweise dazu führen kann, dass der Start des Betriebssystems blockiert wird.

Dateimaske

Darstellung eines Dateinamens mithilfe von Platzhaltern. Die wichtigsten Zeichen in Dateimasken sind * und ? (wobei * für eine beliebige Anzahl von Zeichen steht und ? für ein beliebiges Einzelzeichen).

Datenbank mit bösartigen Webadressen

Eine Liste der Webressourcen, deren Inhalt als gefährlich eingestuft werden kann. Die Liste wird von Kaspersky-Spezialisten erstellt. Sie wird regelmäßig aktualisiert und gehört zum Lieferumfang des Kaspersky-Programms.

Datenbank mit Phishing-Webadressen

Eine Liste der Webressourcen, die von den Spezialisten von Kaspersky als Phishing-Adressen eingestuft wurden. Die Datenbank wird regelmäßig aktualisiert und gehört zum Lieferumfang des Kaspersky-Programms.

Desinfektion von Objekten

Methode zur Bearbeitung von infizierten Objekten, bei der die Daten vollständig oder teilweise wiederhergestellt werden. Nicht alle infizierten Objekte können desinfiziert werden.

Fehlalarm

Eine Situation, in der eine Anwendung von Kaspersky ein nicht infiziertes Objekt als infiziert betrachtet, weil dessen Code dem eines Virus ähnelt.

Gruppenaufgabe

Eine Aufgabe, die einer Administrationsgruppe zugewiesen ist und auf allen verwalteten Geräten innerhalb dieser Gruppe ausgeführt wird.

Gruppenrichtlinie

Siehe Richtlinie.

Infiziertes Objekt

Ein Objekt mit einem Code-Fragment, welches vollständig mit dem Code-Fragment eines bekannten gefährlichen Programms übereinstimmt. Kaspersky-Experten empfehlen, solche Objekte nicht zu verwenden.

Integrationsserver

Die Komponente "Kaspersky Endpoint Security for Virtualization Light Agent". Realisiert die Interaktion zwischen den Komponenten von Kaspersky Endpoint Security und der virtuellen Infrastruktur.

Kaspersky-Update-Server

HTTP- und FTP-Server von Kaspersky, von denen die Anwendungen Datenbanken-Updates und Updates von Modulen der Anwendung erhalten.

Light Agent

Die Komponente "Kaspersky Endpoint Security for Virtualization Light Agent". Wird auf jede virtuelle Maschine, die geschützt werden soll, installiert.

Lizenz

Ein zeitlich begrenztes Nutzungsrecht für eine Anwendung, das Ihnen auf Basis eines Endbenutzer-Lizenzvertrags überlassen wird.

Lizenzzertifikat

Dokument, das Sie zusammen mit einer Schlüsseldatei oder einem Aktivierungscode von Kaspersky erhalten. Dieses Dokument enthält Informationen über die Lizenz, die Ihnen zur Verfügung gestellt wird.

Programm aktivieren

Freischaltung aller Funktionen der Anwendung. Die Anwendung wird vom Benutzer während oder nach der Installation aktiviert. Für die Aktivierung der Anwendung benötigt der Benutzer einen Aktivierungscode oder eine Schlüsseldatei.

Proxy-Server

Ein Netzwerkdienst, mit dem Clients indirekte Anfragen an andere Netzwerkdienste richten können. Der Client baut zunächst eine Verbindung zu einem Proxyserver auf und fordert eine bestimmte Ressource an (z. B. eine Datei), die sich auf einem anderen Server befindet. Dann stellt der Proxyserver entweder eine Verbindung zum angegebenen Server her und ruft die Ressource von dort ab, oder er gibt die Ressource aus dem eigenen Cache zurück (falls der Proxyserver über einen eigenen Cache verfügt). In einigen Fällen kann die Client-Anfrage oder die Antwort des Servers für bestimmte Zwecke vom Proxyserver verändert werden.

Reserveschlüssel

Ein Schlüssel, der das Recht auf Nutzung der Anwendung gewährt, jedoch im Augenblick nicht aktiviert ist.

Richtlinie

Eine Richtlinie bestimmt die Einstellungen für den Betrieb der Anwendung und verwaltet den Zugriff auf die Konfiguration von auf Geräten innerhalb einer Administrationsgruppe installierten Anwendungen. Für jede App muss eine eigene Richtlinie erstellt werden. Sie können eine unbegrenzte Anzahl von unterschiedlichen Richtlinie für eine auf den Geräten der einzelnen Administrationsgruppen installierte Anwendung erstellen. Allerdings kann innerhalb einer Administrationsgruppe pro Anwendung nur eine Richtlinie gleichzeitig angewendet werden.

Schutz vor Verschlüsselung

Bösartige Aktivitäten von Verschlüsselungsprogrammen, die auf die Verschlüsselung von Dateien mit Benutzerdaten abzielen. Verschlüsselte Dateien sind weder lesbar noch verwendbar.

SIEM-System

Security Information and Event Management-System. Eine Lösung, mit der Informationen und Ereignisse im Sicherheitssystem eines Unternehmens verwaltet werden.

SVM

Eine Secure Virtual Machine (SVM) ist eine spezielle virtuelle Maschine, auf welcher der Dienst "scanserver" (Dienst des Schutzservers als Komponente von Kaspersky Endpoint Security for Virtualization Light Agent) installiert ist.

Vertrauenswürdiges Gerät

Ein Gerät, auf das Benutzer, die in den Einstellungen des vertrauenswürdigen Geräts festgelegt wurden, jederzeit vollständigen Zugriff haben.

Informationen über den Code von Drittherstellern

Informationen über den Code von Drittherstellern finden Sie in der Datei legal_notices.txt, die sich im Installationsordner der Anwendung befindet.

Markenrechtliche Hinweise

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

AMD64 ist ein Markenzeichen oder eingetragenes Markenzeichen von Advanced Micro Devices, Inc.

Amazon ist ein Markenzeichen von Amazon.com, Inc. oder seinen verbundenen Unternehmen.

Mac und FireWire sind Markenzeichen von Apple Inc.

Arm ist ein eingetragenes Markenzeichen von Arm Limited (oder seinen Tochtergesellschaften) in den Vereinigten Staaten und/oder anderen Ländern.

Die Bluetooth-Wortmarke, das Markenzeichen und die Bluetooth-Logos sind Eigentum von Bluetooth SIG, Inc.

Ubuntu und LTS sind eingetragene Markenzeichen von Canonical Ltd.

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 und Google Public DNS sind Markenzeichen von Google LLC.

HUAWEI, EulerOS und FusionSphere sind Markenzeichen der Huawei Technologies Co., Ltd.

Intel und Core sind Markenzeichen der Intel Corporation oder ihrer Tochtergesellschaften.

Linux ist ein in den USA und/oder in anderen Ländern eingetragenes Markenzeichen von Linus Torvalds.

Microsoft, Active Directory, Hyper-V, Outlook, Visual C++ und Windows sind eingetragene Markenzeichen der Microsoft-Unternehmensgruppe.

OpenStack ist ein eingetragenes Markenzeichen der OpenStack Foundation in den USA und anderen Ländern.

Oracle und JavaScript sind eingetragene Markenzeichen des Unternehmens Oracle und/oder von verbundenen Unternehmen.

Python ist ein Markenzeichen oder eingetragenes Markenzeichen der Python Software Foundation.

Red Hat, Red Hat Enterprise Linux, CentOS und Fedora sind Markenzeichen und/oder sind in den USA und anderen Ländern eingetragene Markenzeichen von Red Hat, Inc. oder seinen Tochterunternehmen.

Debian ist ein eingetragenes Markenzeichen von Software in the Public Interest, Inc.

SUSE ist ein in den USA und in anderen Ländern eingetragenes Markenzeichen von SUSE LLC.

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.